RUTGERS
BIOMEDICAL AND
HEALTH SCIENCES

Policy Name: Information Classification

Approval Authority: Senior Vice President for Finance and Administration

Originally Issued: July 1, 2013

Revisions:

1. **Who Should Read This Policy**

This policy applies to any individual responsible for the management, operation, and/or maintenance of the legacy UMDNJ information technology services and/or environment. If you are uncertain whether this policy applies to you, please contact your direct supervisor.

2. **Related Documents (refer to policies.rutgers.edu for additional information)**

Family Educational Rights and Privacy Act (FERPA) 20 U.S.C. 1232g; 34 CFR Part 99
Federal Information Security Management (FISMA) Act
http://csrc.nist.gov/groups/SMA/fisma/index.html
Federal Trade Commission http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml
Health Insurance Portability and Accountability Act of 1996
http://www.hhs.gov/ocr/privacy/index.html: Sections: 164.308 (a) (4) (ii) (B), 164.308 (a) (4) (ii) (C), 164.308 (a) (7) (ii) (E), 164.312 (e) (1), 164.312 (e) (2)
New Jersey Open Public Records Act Section: N.J.S.A. 47:1A-1.1
New Jersey Identity Theft Prevention Act Sections: N.J.S.A. 56:8-161, N.J.S.A. 56:8-163
Payment Card Industry Sections: PCI DSS v2 7.1, PCI DSS v2 7.2

3. **The Policy**

All members of the University community have a responsibility to protect the confidentiality, integrity, and availability of information collected, processed, transmitted, stored, or transmitted by the University, irrespective of the medium on which the information resides.

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

information, student records, and personally identifiable information), the protection levels must satisfy the data security and data privacy requirements.

I. Requirements:

A. President/CEOs, Vice Presidents and Deans must:

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

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

3. Assign business unit managers, senior managers, or designees the role of Information Owner for their respective areas.

4. Ensure that their Information Owners maintain an inventory of their information assets, including applications.

5. Annually perform a risk assessment of their applications.

6. Annually report their aggregate inventory of information assets to OIT.

B. Information Owners must:

1. Classify University information under their control as (reference the EXHIBIT):

- CONFIDENTIAL
- PRIVATE
- INTERNAL
- PUBLIC

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

2. Where practicable, clearly label Confidential and Private information.

3. Establish its criticality using the Department of Risk Management and Insurance's Business Impact Analysis methodology.

4. Establish the business unit's security requirements and expectations for the applications the business unit owns and which contain their information. For example:

a. How a user should be authenticated
b. How users will be granted access to the application.
c. Revocation procedures of user access privileges
d. Procedures for approving requests for access and use of the information in its applications
e. Record retention and e-discovery requirements.

5. Maintain an inventory of their information assets, including all applications that collect, process, transport, store, or transmit their information. (The Department of Risk Management and Insurance's business impact analysis methodology can assist with this effort.)

6. At minimum, annually assess and update the Information Classification, based on changing usage, sensitivities, law, or other relevant circumstances. Changes must be reported to their business unit's VP or Dean and the application managers.

7. Establish procedures for data destruction in accordance with the University's records retention and disposal policies.

C. Confidential and Private Information must be collected, processed, transported, stored, or transmitted using only:

1. Software, hardware, and services whose security is managed by the University (e.g., remote access services, University messaging services, applications, databases, and servers managed by a local school/unit technology organization or OIT).

2. Third Party managed devices or services that are subject to a contract between the Third Party and the University that contains confidentiality provisions consistent with University policies and standards.

D. External Handling/Security Requirements:

University information in electronic form that is regulated by Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), or Payment Card Industry (PCI) must be encrypted when electronically stored, transmitted, or transported externally.

Information entrusted to the University by grant-providers or the National Institutes of Health (NIH) (data-sharing arrangements) must be protected, at minimum, according to contractual obligations, regulatory requirements, and/or University policy, and relative to the sensitivity of the information.

Information Owners may establish similar security requirements for non-regulated information at their discretion.

E. Internal Handling/Security Requirements:

Information regulated by HIPAA, FERPA, GLBA, or PCI that is stored on removable media must be encrypted at all times, even when the information is stored or transported within the University's campus.

Information entrusted to the University by grant-providers or NIH (data-sharing arrangements) must be protected, at minimum, according to contractual obligations, regulatory requirements, and/or University policy, and relative to the sensitivity of the information.

F. Prohibited Actions (include, but are not limited to):

All members of the Rutgers community must NOT:

1. Forward University information classified as Confidential or Private to outside or personal email accounts. (They MAY exchange information via email with authorized third parties, using the university's messaging services.)

2. Use services OTHER than the University's remote access or web portal services to remotely conduct University business that is considered sensitive.

3. Use devices or services OTHER than University-managed devices or services to collect, process, transport, store, or transmit Confidential or Private information. (Personal smartphones and removable media that are secured by the University are considered “University-managed.”)

4. Discuss or post information classified as Confidential, Private, or Internal on social networks (e.g., MySpace, Facebook, LinkedIn), blogs, or any other medium not directly managed by the University and without the explicit consent of management, Legal, and Compliance.

5. Discuss or share information classified as Confidential or Private with unauthorized parties, including University personnel, regardless of format.

II. Responsibilities:

All members of the Rutgers community must protect the confidentiality, integrity, and availability of University information, regardless of format.

A. Vice Presidents and Deans must exercise due care and control of their school and unit information assets by ensuring compliance with this policy, legal requirements, and fulfilling the specific duties specified in the section on requirements.

B. Information Owners must:

1. Implement this policy.

2. Fulfill the specific duties specified in the section on requirements.

3. Provide training and awareness about information handling to users with access to their Confidential and Private information.

4. Annually assess the information classification, criticality, and risk of their information assets, and update it accordingly.

C. OIT/Local Technology Organization must implement the technical security requirements defined by the Information Owner.

III. Information Security Incident Reporting

Unauthorized disclosure, loss or theft of Confidential or Private information must be reported immediately. The following steps must be taken:

1. Immediately report loss, theft, or unauthorized access to a manager. If the information is Electronic Patient Health Information (ePHI), Compliance must be notified.

2. Report loss or theft of physical assets to the Department of Risk Management and Insurance.

IV. 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.

V. Exhibit

Information Classification Table

EXHIBIT
Information Classification Table

Information Classification	Description	Examples	Encryption Requirements
Confidential	The most sensitive information, which requires the strongest safeguards to reduce the risk of unauthorized access or loss. 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/HITECH penalties).	• Bank/Financial information • Login Credentials (username & password) • Credit/Debit Card Number • Driver's License Number • Human Resources information if it contains SSNs, medical reports. • Passport Number • Patient Health Care Information[1] • Protected Data Related to Research[2] • Social Security Number • Student Disciplinary, or Judicial Action Information • University Financial Data on Central Systems	1. When electronically transmitted externally: a. Email b. Business-to-Business (B2B)* c. Web session *B2B: Electronic Data Interchange (EDI); between the University and contractual partners. 2. When stored or transported on mobile computing devices or removable media. 3. Outbound (i.e., sent to external parties) EPHI information: e.g. (provided by the American Medical Association) electronic medical records; documents containing EPHI; claims payment appeals; scanned images, such as copies of remittance advices; emails containing EPHI; and claims sent to a clearinghouse. 4. Databases containing Credit/Debit Card, at minimum the PAN must be rendered unreadable anywhere it is stored.
Private	Sensitive information that is restricted to authorized personnel and requires safeguards, but which does not require the same level of safeguards as confidential information. Unauthorized disclosure or access may present legal and reputational risks to the University.	• Human Resources Data listed on N.J.S.A. 47:1A-1.1 as excluded from public records. (Medical data and SSNs are treated as Confidential.) • Sensitive Business Information[3] • Student Academic Information • Student Examination Questions	1. When electronically transmitted externally: a. Email b. B2B c. Web session 2. When stored or transported on removable media.

EXHIBIT (continued)
Information Classification Table

Information Classification	Description	Examples	Encryption Requirements
Internal	All other non-public information not included in the Confidential or Private classes	• Licensed Software • Other University Owned Non-Public Data • University Identification Number or Information Number (employee numbers, student ID numbers, etc.)	Suggested, but not required.
Public	All public information.	General access data, such as that on unauthenticated portions of ~~www.umdnj.edu~~ **www.rutgers.edu**	Not required.

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

- Patient Health Information (PHI) or Electronic Patient 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
- National Practitioner Data Bank information

[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

[3]Sensitive Business Information

Certain business records such as business plans containing competitive information; management memos discussing proposed policies; audit information; contract negotiation strategies.