Information Classification

ROWAN UNIVERSITY POLICY

Title: ***Information Classification Policy***
Subject: *Information Security*
Policy No: *ISO:2013:08*
Applies: University-Wide
Issuing Authority: *Senior Vice President for Information Resources and Technology and Chief Information Officer*
Responsible Officer: Director of Information Security
Adopted: 07/01/2013
Amended: 06/01/2014
Last Revision: 07/02/2018

I. PURPOSE

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 the University's information receives appropriate and consistent levels of protection to safeguard its Confidentiality, Integrity, and Availability.

II. ACCOUNTABILITY

Under the direction of the President, the Chief Information Officer and the Director of Information Security shall implement and ensure compliance with this policy. The Vice Presidents, Deans, and other members of management will implement this policy in their respective areas.

III. APPLICABILITY

This policy applies to all members of the Rowan community including faculty, staff, non-employees, students, attending physicians, contractors, covered entities, and agents of Rowan, as well as visitors, who have been explicitly and specifically authorized to access and use the University's information systems.

IV. DEFINITIONS

1. *Application* – A computer program that processes, transmits, or stores University information and which supports decision-making and other organizational functions. It typically presents as a series of records or transactions. These records and transactions are generally accessible by more than one user.
2. *Application Manager* – the technology manager who is directly responsible for the development, maintenance, configuration, or functional specifications of the application. He or she is also required to implement, operate, and maintain security measures defined by the information owners.
3. Authorized User – a person authorized to access information resources specific to their role and responsibilities, and who has conveyed upon them the expectation of "Least Privilege."
4. Business (Application) Owner – business unit that purchased the application using University funds allocated to its budget or purchased using a grant. The business owner may be a technology organization for utility services-type applications, such as Banner and MS Exchange.
5. *Business Unit* – the term applies to multiple levels of the university, such as a revenue generating unit or functional unit (e.g., Compliance, Human Resources, IRT, Legal). It may also be comprised of several departments.
6. *Business-Critical Function/Process* – a function or process which, if compromised, presents a severe financial, operational, or regulatory risk to the business unit and/or to the University as a whole. A

business-critical function/process may be supported by an information system owned by the business unit or by an information system that is shared across multiple units.

7. *Business Impact Analysis (BIA)* – a process managed by the Office of Emergency Management that determines the financial and operational impact of a disruption to a business, and the requirements for recovering from the disruption. A business unit uses the BIA to list their business-critical functions and processes and supporting applications.
8. *Confidential Information* – 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 Rowan University to legal risk, 2) adversely affect its reputation, 3) jeopardize its mission, and 4) present liabilities to individuals (for example, HIPAA/HITECH penalties). See EXHIBIT for additional clarification.
9. *Due Care* – steps that demonstrate the University has taken responsibility for the activities that take place within the institution, and has implemented the requisite measures to help protect its assets, including its students, faculty, staff, and the community which we serve.
10. *Information Asset* – application, database, network, or body of information that is of value and importance to the University.
11. *Encryption* – method of converting information or data into a cipher or code to prevent unauthorized access. Requires a pass code or other form of confirming identity to decrypt and access the information or data.
12. *EPHI* – Electronic Protected Health Information
13. *External Data* – data for which the University is a custodian, such as video or media that are not directly licensed to Rowan University, but are being offered to the Rowan community via an external partnership.
14. *FERPA* – Family Educational Rights and Privacy Act. A Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA applies to the records of individuals from the point of first registration until death of the individual.
15. *GLBA* – Gramm-Leach-Bliley Act. Requires academic institutions to implement policies and controls for protecting financial information. An institution that is compliant with FERPA is considered compliant with GLBA.
16. *HIPAA* – Health Insurance Portability and Accountability Act of 1996
17. *Information Asset* – application, database, or body of information that is of value to the University.
18. *Information Owner* – information owners are the business unit mangers, senior management, or their designees who have planning and management or legal responsibility for the information generated within their functional areas. They must ensure that the level of protection assigned to their information is relative to its classification and sensitivity. For information regulated by HIPAA, FERPA, or GLBA, the information owner is expected to exercise due care when defining its level of protection.
19. *Information Risk* – the potential that a given threat will exploit vulnerabilities of an information asset, thereby causing loss or harm to the information asset. It is measured in terms of a combination of the probability of an event and its impact to the University if the confidentiality, integrity, or availability of an asset is compromised. A risk can be financial, operational, regulatory, and/or reputational in nature.
20. *Internal Information* – data that is owned by the University, is not classified Confidential or Private, and is not readily available to the public. For example, this includes employee and student identification numbers and licensed software.
21. *Least Privilege* – giving every user, task, and process the minimal set of privileges and access required to fulfill their role or function. This includes access to information systems and facilities.
22. *Mobile Computing Device* – including, but not limited to, laptops, netbooks, smartphones (Blackberry, iPhone, etc.) and mobile broadband cards (also known as AirCards® and connect cards).
23. *NIH* – National Institutes of Health.
24. *PAN* – Credit Card Primary Account Number.
25. *PCI* – Payment Card Industry.
26. *Private Information* – 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. See Exhibit A for additional clarification.
27. *Public Information* – information that is readily available to the public, such as the information published on web sites.

28. *Removable Media* – including, but not limited to, CDs, DVDs, copier hard drives, storage tapes, flash devices (e.g., CompactFlash and SD cards, USB flash drives), and portable hard drives.
29. *Risk Assessment* – a process used to identify and evaluate risks and their potential impact on the University.

V. REFERENCES

A. Acceptable Use Policy ISO: 2013:01

B. Mobile Computing and Removable Media Policy ISO: 2013:02

C. Family Educational Rights and Privacy Act (FERPA) 20 U.S.C. 1232g; 34 CFR Part 99

D. Federal Information Security Management Act (FISMA) http://csrc.nist.gov/groups/SMA/fisma

E. Federal Trade Commission http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml

F. 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)

G. New Jersey Open Public Records Act Section: N.J.S.A. 47:1A-1.1

H. New Jersey Identity Theft Protection Act Sections: N.J.S.A. 56:8-161, N.J.S.A. 56:8-163

I. Payment Card Industry Sections: PCI DSS v2 7.1, PCI DSS v2 7.2

VII. POLICY

A. 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 the University's 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 when needed.

B. 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.

C. Vice Presidents and Deans shall:

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 Data Steward for their respective information.

4. Ensure that their Data Stewards 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 the Information Security Office.

D. Data Stewards shall:

1. Classify University information under their control as (reference the Definitions Section and EXHIBIT):
    a. CONFIDENTIAL
    b. PRIVATE
    c. INTERNAL
    d. 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 Office of Information Security'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 ISO'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 record retention and disposal policies.

E. Confidential and Private information must be collected, processed, transported, stored, or transmitted using <u>only</u>:

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 IRT).
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.

F. External Handling/Security Requirements:

1. University information in electronic form that is regulated by HIPAA, FERPA, GLBA, or PCI must be encrypted when electronically stored, transmitted, or transported externally.
Information entrusted to the University by grant-providers or NIH (data-sharing arrangements) must

be protected, at a minimum, according to contractual obligations, regulatory requirements, and/or University policy, and relative to the sensitivity of the information.
2. Data Stewards may establish similar security requirements for non-regulated information at their discretion.

G. Internal Handling/Security Requirements:

1. 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.
2. 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.

H. Prohibited Actions (include, but are not limited to):
All members of the Rowan 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.

VII. NON-COMPLIANCE SANCTIONS

Violation of this policy may subject the violator to disciplinary actions, up to or including termination of employment or dismissal from a school, and may subject the violator to penalties stipulated in applicable state and federal statutes.

By Direction of the CIO:

Mira Lalovic-Hand,

SVP and Chief Information Officer