RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

~~RUTGERS~~ UNIVERSITY 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~~

Policy Name:	Information Classification				
Section #:	70.1.2	**Section Title:**	Information Technology: Information Technology Policies	**Formerly Book:**	00-01-95-15 (Legacy UMDNJ); Policy 70.2.2
Approval Authority:	Executive Vice President – Chief Financial Officer and University Treasurer	**Adopted:**	~~07/01/2013~~	**Reviewed:**	~~04/06/2021~~
Responsible Executive:	Senior Vice President & Chief Information Officer	**Revised:**	10/10/2013 (updated title); 07/03/2014 (significant updates); 06/30/2018 (significant updates); 04/06/2021		
Responsible Office:	Office of Information Technology (OIT)	**Contact:**	oit-policies@oit.rutgers.edu		

1. **Policy Statement**

This policy outlines the standards for classifying information at Rutgers, The State University of New Jersey. Classification categories (Critical, 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**

This policy applies to all ~~-~~members of the University community including faculty, staff, students, covered entities, contractors, non-employees, and agents of the University.

Parties with major responsibilities include Executive/Senior/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. **Resources**

~~**Related Documents**~~

University Policy: Information Technology - Section 70

University Policy: Clinical, Compliance, Ethics & Corporate Integrity - Section 100

University Policy 30.4.5: Records Management

~~Policies.rutgers.edu: Information Technology - Section 70~~
~~Policies.rutgers.edu: Clinical, Compliance, Ethics & Corporate Integrity - Section 100~~
University Policy 40.2.15: Payment Card Acceptance Policy

University Policy 50.3.7: Copyright Policy

~~University Policy 50.3.18: Data Breach Management~~

~~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~~
University Policy 50.3.11: Gramm-Leach-Bliley Act (GLBA) Information Security Policy

University Policy 50.3.12: Red Flag Detection and Reporting Policy

University Policy 50.3.18: Data Breach Management

University Policy 70.1.3: Incident Management

~~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
~~https://it.rutgers.edu/it-risk-policy-and-compliance/knowledgebase/minimum-security-standards-for-data-protection/~~

~~http://rusecure.rutgers.edu/policies~~

5. **Definitions~~Contacts~~**

Availability - The expectation that information is accessible by the University community when needed.

Confidentiality ~~-The expectation that only authorized individuals, processes, and systems will have access to University information~~ The state of keeping information and/or materials private, with only authorized individuals, processes, and systems having access to view, use, or share.

Guidelines - Advice on the ways to comply with policy, written for non-technical users who have multiple options for secure information handling processes.

Integrity - The expectation that the University's information will be protected from intentional, unauthorized, or accidental changes.

Information Owner - An organizational official with statutory, management, or operational authority for specified information who is responsible for establishing the procedures governing its generation, collection, processing, dissemination, and disposal. (National Institute Standard (NIST) 800-12)

Procedures – Step-~~-~~by-~~-~~step instructions and implementation details for personnel to perform specific tasks in ways that ensure that the associated preventive, detective, and/or response mechanisms work as planned.

Technology standards - Established requirement of technical configuration parameters and associated values to ensure that management can secure U~~u~~niversity assets and comply with U~~u~~niversity policy and regulatory requirements. It is a formal document that establishes uniform engineering or technical criteria, methods, processes, and practices.

Top Secret, Secret, and Confidential - C~~are c~~lassifications of the United States federal government ~~and~~ which retain security requirements separate from this policy.

~~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., Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA)).

B. **Requirements:**

1. **Executive/Senior/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~~ Critical 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. Ensure a~~A~~nnual~~ly perform a~~ risk assessments of their applications are performed for their business units ~~and data~~. Critical data that have ~~For areas with~~ specific compliance and regulatory requirements ~~such as HIPAA and GLBA, business units~~ must also be reported ~~their aggregate inventory of information assets~~ to ~~OIT Information Protection and Security~~IT Risk, Policy and Compliance.

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

~~e.~~f. Ensure the proper and effective use of encryption to protect the confidentiality, authenticity, and integrity of information classified as Critical or Restricted especially with regard to mobile computing devices, removable media, and to the electronic transmission of such information.

2. **Information Owners ~~(data custodians)~~ must:**

a. Classify University information under their control as:

- Critical
- Restricted

~~•~~ Internal

-
- Public

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

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

~~———~~Clearly identify Critical, Restricted, and Internal Information, especially when sharing or providing individuals, departments, or third parties with access.

b.

Establish ~~the business unit's~~ security requirements and expectations for the applications which are owned by or contain information for the business unit. ~~owns and which contain their information.~~

~~c. 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.~~c. Provide training and awareness ~~about~~ on information handling to users with access to ~~their Restricted~~ Critical ~~Information~~data.

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

~~f.~~e. Conduct an annual entitlement review of individuals, departments, and third parties who have been granted access to ~~Restricted~~ information based on Information Classification.

~~g.~~f. At minimum, annually assess and update the Information Classification~~,~~ assigned to their data based on changing usage, sensitivities, law, or other relevant circumstances.

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

~~i.~~h. 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~~ or 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).

i.

j. 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 ~~s~~State, federal, and contractual requirements that may apply.

~~k. See the Related Documents Section for further information.~~

k. Establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance as stated in this Policy. This includes, but is not limited to establishing the rules for the appropriate use and protection of the subject information. [National Institute of Standards and Technology Special Publication 800-12]

3. **Information Users must:**

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

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

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

d. ~~Apply~~ Ensure that their IT support staff have applied controls that meet the **"**Rutgers Minimum Security Standards for Data Protection" as appropriate based on the ~~data~~ Information C~~c~~lassification (e.g. Critical and Restricted data must be encrypted on mobile devices, removable media, and when transmitted).~~.~~

4. **External Data Handling Security Requirements**:

Information entrusted to the University by grant-providers, other universities, or other agencies (Department of Defense (DoD), National Endowment for the Humanities (NEH), National Institutes of Health (NIH), National Science Foundation (NSF) or similar) and companies must be protected, at minimum, according to contractual obligations, regulatory requirements, and/or University policy, and relative to ~~the sensitivity of the i~~Information Classification.

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

a. No Critical, Restricted, or Internal information may be provided outside of the department or outside of the U~~u~~niversity 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."~~ University Critical, Restricted, and Internal information provided to outside or third party service providers must be protected by the third party at the Information Classification level. A HIPAA Business Associates Agreement is required if the third party is to receive data classified as Critical.

~~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. ~~C~~ **Information Security Incident Reporting**

Any u~~U~~nauthorized use, disclosure, loss, or theft of Critical, Restricted, or Internal information is a potential breach and must be reported immediately. Refer to University Policy 70.1.3: Incident Management and University Policy 50.3.18: Data Breach Management for reporting requirements.

~~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 S~~s~~tate 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://it.rutgers.edu/it-risk-policy-and-compliance/knowledgebase/minimum-security-standards-for-data-protection/~~
~~https://rusecure.rutgers.edu/content/minimum-security-standards-data-protection~~

Information Classification	Description	Examples
Critical	Critical data is the most sensitive information and requires the highest level of protection. This information classification is intended exclusively for protected health information (PHI) and electronic protected health information (ePHI). University entities that are authorized to use this classification must ensure appropriate coverage, identify and inventory protected information, and implement safeguards in accordance with HIPAA/HITRUST security requirements during the complete life cycle of this data and associated systems.	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~~healthcare 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. • Information labeled by Federal Information Security Management Act (FISMA) or by the National Institute of Standards and Technology Special Publication 800-53
Restricted	Restricted Data is the most sensitive information for non-PHI 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 the University is required to protect under regulatory or legal requirements. Unauthorized disclosure or access may: 1) subject ~~Rutgers~~ the University to legal risk~~,~~; 2) adversely affect its reputation~~,~~; 3) jeopardize its mission~~,~~; and 4) present liabilities to individuals (for example, HIPAA penalties).	• Social Security Number • Bank information • Login Credentials (username & password) • Credit/Debit Card Number • Driver's License Number • Human Resources information if it contains social security numbers (SSNs), medical reports, etc. • Passport Number • ~~Protected Health Care Information (PHI)1~~ • Protected Data Related to Research~~2~~ • 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 • ~~Social Security Number~~ • Student Disciplinary ~~,~~or Judicial Action Information • Police Records • Information labeled as Controlled Unclassified Information (CUI) ~~or~~ by National Institute of Standards and Technology Special Publication 800-171 • Gramm-Leach-Bliley Act (GLBA) information • Payment Card Industry (PCI) information~~Student Records (FERPA)~~ •

~~All regulations and procedures are subject to amendment.~~

Information Classification	Description	Examples
Internal	All other non-public information not included in the Critical or Restricted category.	• Student Records labeled by Family Education Rights and Privacy Act (FERPA) • Licensed Software • Other University-Owned Non-Public Data • University Identification Number or Information Number (e.g. employee numbers, student ID numbers, etc.)
Public	All public information.	General access data, such as that on unauthenticated portions of any rRutgers.edu website.

[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