1. **Policy Statement**
   This policy outlines the standards for classifying information at Rutgers, The State University of New Jersey. Classification categories (confidential, private, internal and public, 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 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. 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**
   c. Federal Trade Commission
A. Introduction:

All members of the University community have a responsibility to protect the confidentiality, integrity, and availability of University information collected, processed, transmitted, stored, or transmitted by the University, 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 Rutgers University information.
- Integrity – the expectation that Rutgers the University’s information will be protected from intentional, unauthorized, or accidental changes.
- Availability – the expectation that information is accessible by Rutgers 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 protected health information, student records, and 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. President/CEOs, 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 sensitive Restricted information.

c. Assign business unit managers, senior managers, or designee 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 that their Information Owners 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. Annually report their aggregate inventory of information assets to OIT. 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 (reference the EXHIBIT):

• CONFIDENTIAL
• PRIVATE
• 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. Where practicable, clearly label Confidential and Private information. Clearly identify Restricted and Internal Information specially when sharing or providing individuals, departments or third parties with access.

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

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, transport, store, or transmit their information. (The Department of Risk Management and Insurance’s business impact analysis methodology can assist with this effort.)

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. Changes must be reported to their business unit’s VP or Dean and the application managers.

h. Establish procedures for data destruction in accordance with the University’s records retention and disposal policies. See policy 50.3.10 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.) Confidential and Private Information must be collected, processed, transported, stored, or transmitted using only: Information Users must:

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.

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:

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) 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.

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

5.) Internal Handling/Security Requirements: Data provided to External (third party) Services:

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.

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.

6.) 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.

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.

C Information Security Incident Reporting

Unauthorized use, disclosure, loss or theft of Restricted or Internal Confidential or Private 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, unauthorized access to a manager. If the information is Electronic Patient Health Information (ePHI), Compliance must be notified.

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 the Department of Risk Management and Insurance 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. Exhibit Appendix

Information Classification Table
## EXHIBIT
### Information Classification Table

<table>
<thead>
<tr>
<th>Information Classification</th>
<th>Description</th>
<th>Examples</th>
<th>Encryption Requirements</th>
</tr>
</thead>
</table>
| 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  
- Protected Data Related to Research  
- 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  
- 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

<table>
<thead>
<tr>
<th>Information Classification</th>
<th>Description</th>
<th>Examples</th>
<th>Encryption Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal</td>
<td>All other non-public information not included in the Confidential or Private classes</td>
<td>• Licensed Software &lt;br&gt;• Other University Owned Non-Public Data &lt;br&gt;• University Identification Number or Information Number (employee numbers, student ID numbers, etc.)</td>
<td>Suggested, but not required.</td>
</tr>
<tr>
<td>Public</td>
<td>All-public information.</td>
<td>General access data, such as that on unauthenticated portions of <a href="http://www.rutgers.edu">www.rutgers.edu</a></td>
<td>Not required.</td>
</tr>
</tbody>
</table>

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.
## 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-electronic-devices](https://rusecure.rutgers.edu/content/minimum-security-standards-electronic-devices)

[https://rusecure.rutgers.edu/content/minimum-security-standards-data-protection](https://rusecure.rutgers.edu/content/minimum-security-standards-data-protection)

<table>
<thead>
<tr>
<th>Information Classification</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| 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 Research²  
• 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.            |

¹Protected 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

²Protected Data Related to Research

• University propriety 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

All regulations and procedures are subject to amendment.

Page 10 of 10