



**New Jersey Institute of Technology  
University Policies and Procedures**

**Date of Issue: June 13, 2022**

***Subject: Data Classification Policy***

## **I. POLICY STATEMENT**

This policy establishes standards for classifying University Data (as defined herein) according to its sensitivity levels, legal requirements, and the nature of its confidentiality while maintaining the integrity and availability of the data. These classifications will provide guidance to the University community on how to manage, handle, maintain, store, use and access data in compliance with applicable federal and state laws and regulations, as well as other University policies. As such, this policy applies to all University faculty members, students, staff members, agents, contractors, visitors, and any person to whom NJIT has provided access to University Data, information resources and assets.

The protection of University Data needs to be done in compliance with all applicable laws and regulations. The policy imposes two requirements in furtherance of those objectives. First, the Information Services & Technology (IST) Division shall develop minimum security standards for each class of data, implement security controls, and provide support to the University community to help them adhere to these standards. Second, members of the University community, who are entrusted with University Data, must familiarize themselves with these Minimum Security Standards (as defined herein), as well as the associated risks related to the unauthorized disclosure, alteration or destruction of University Data.

## **II. DEFINITION**

- **Data:** Any information that has been collected, observed, generated or created for reference or analysis. Data, as a definition, is very broad and includes information used in teaching, research, and administration, and may be preserved in any medium, including, but not limited to electronic files and paper documents. Data include original documents as well as all backup and duplicate copies.
- **University Data:** Data created or received by *data users* while acting on behalf of NJIT, or data created or received by NJIT students, faculty, staff, researchers, or any person or group while providing a service to NJIT or to others as part of their education or training. University data does not include intellectual property which by law or by NJIT's copyright is owned, licensed, or otherwise legally controlled by a Data User.
- **Data User:** University departments or individual University community members who have been granted access to University Data in order to perform assigned duties or in fulfillment of assigned roles or functions within the University.

- **Minimum Security Standards:** Standards that describe the minimum controls required to secure and protect University Data. These standards vary based upon data classification and apply to all data classifications other than public data. See Appendix A.

### III. DATA CLASSIFICATION

NJIT's University Data is classified into four categories, as further set forth in Appendix B, which are determined by the sensitivity level of the data and the risks associated with data disclosure and/or loss.

- **Restricted:** Data is classified as restricted when the unauthorized disclosure, alteration or destruction of that data could be a high risk to University or its affiliates, causing the University a significant adverse impact. Restricted data, in many instances, are also required to be protected by federal or state laws or regulations. Examples of Restrictive data:
  - Student Educational Records subject to the Family Educational Rights and Privacy Act (FERPA), including but not limited to transcripts.
  - Social Security Number
  - Passport Number
  - Driver's License Number
  - Protected Health Information (PHI) and data covered by the Health Insurance Portability and Accountability Act (HIPAA)
  - Bank/Financial/Credit Card Account Numbers
  - University Financial Data
  - University Research Data, i.e. Export Controlled data, ITAR/CUI
  - Litigation related information and privileged legal communications
  - Police Records
- **Sensitive:** Data is classified as sensitive if the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the University or its affiliates. Examples of Sensitive data:
  - Login credentials - UCID and password
  - Non-public business communications, emails, and internal memos, including related non-public documents and forms
  - Any non-public student, personnel or alumni bio data not covered by Restricted
  - University Intellectual Property
  - University sponsors and donors' information
  - Employees home addresses and personal phone numbers or personal email addresses
  - Directory information for employees who have requested non-disclosure

- Directory information for students who have requested non-disclosure under FERPA
- **Internal:** Data is classified as Internal if the unauthorized disclosure, alteration or destruction of that data could result in a low level of risk to the University or its affiliates. Examples of Internal data:
  - Licensed Software
  - NJIT ID number (employee ID, student ID)
  - Directory information for employees who have not requested non-disclosure
  - Web-based resources designed for non-Public University use
  - Directory Information for students who have not requested non-disclosure under FERPA (i.e., [directory.njit.edu](http://directory.njit.edu), name, telephone)
- **Public:** Data that is readily available to the public, and/or classified as public information under the New Jersey Open Public Records Act, and can be disclosed without special authorization. Public data needs no additional protection. Examples of Public data:
  - UCID
  - Course Catalog
  - Employee Directory Information
  - Publicly Accessed Websites
  - Publicly Accessed Research Data (at data owner's discretion)
  - Press Releases
  - Board of Trustee Resolutions and Public Meeting Minutes

Users of data that is classified as restricted, sensitive, or internal must follow the safeguards outlined in NJIT's minimum security standards.

The categorization of the University Data is not indicative of the scope and nature of documents which may be produced pursuant to the State of New Jersey's Open Public Records Act (N.J.S.A. 47:1A-1 et seq.).

#### IV. DATA HANDLING

- **Partnerships with Outside Agencies:** As a public research university, faculty and staff may partner with outside agencies such as the Department of Defense (DoD), National Institutes of Health (NIH), and National Institute of Environmental Health Sciences (NIEHS), and other agencies. In these cases, additional data handling requirements may be applied according to contractual obligations, regulatory requirements, policies, and/or related to data classification. All members of the University community that work with outside agencies need to be aware of and abide by relevant obligations.

- **Data provided to third party services:** Any data provided to third party services needs to be protected, at a minimum, in such a way that meets the data classification requirements. Data which has been categorized as Restricted, Sensitive, or Internal may not be provided to outside third parties without a written agreement in place which has been reviewed and approved by NJIT's Office of General Counsel.

## **V. INCIDENT REPORTING**

Any potential data breach of Restricted, Sensitive, or Internal data must be reported immediately as outlined in NJIT's Data Incident Response plan. A potential data breach includes but is not limited to unauthorized use, disclosure, loss, or theft of the data.

## **VI. COMPLIANCE**

University Data resources are the property of or licensed to NJIT and are provided to the University community as either a limited privilege or a direct responsibility. Any violations to this policy may result in denial or removal of access privileges to the University's electronic systems, and potential disciplinary action under applicable University policies and procedures.

## **VII. UPDATES**

The Enterprise Analytics Governance Committee, with input from the Data Governance Subcommittee, will periodically review the Data Classification policy. As such, this policy may be updated accordingly.

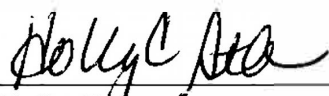
## **VIII. ADMINISTRATION**

Under the direction of the Office of the Provost, this policy will be administered by the Enterprise Analytics Governance Committee with support of University stakeholders.

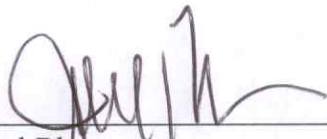
### **EFFECTIVE DATE OF POLICY**

This policy takes effect upon adoption, and supersedes and revokes any former policies governing the subject matter.

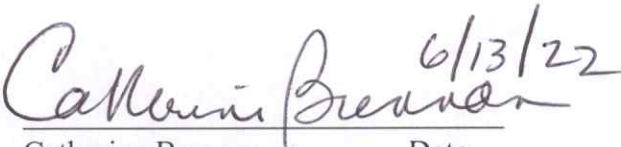
### **REVIEW:**

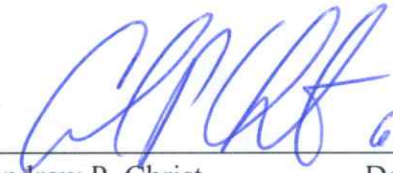
 6/13/22  
\_\_\_\_\_  
Holly C. Stern, Esq.                      Date  
General Counsel  
Vice President for Legal Affairs

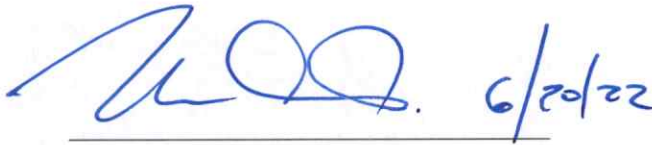
**APPROVAL:**

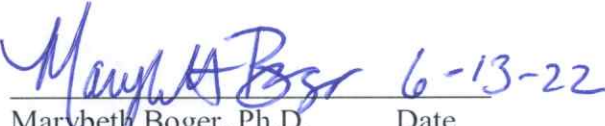
  
\_\_\_\_\_  
Joel Bloom                      Date  
President                      6/15/22

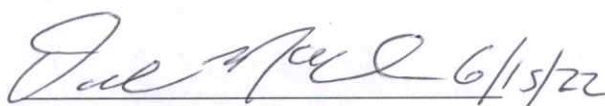
  
\_\_\_\_\_  
Fadi P. Deek                      Date  
Provost & Senior Executive Vice President                      6/13/2022

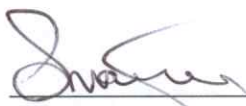
  
\_\_\_\_\_  
Catherine Brennan                      Date  
Senior Vice President for Finance and                      6/13/22  
Chief Financial Officer

  
\_\_\_\_\_  
Andrew P. Christ                      Date  
Senior Vice President for Real Estate                      6-13-22  
Development & Capital Operations

  
\_\_\_\_\_  
Kenneth Alexo, Jr., Ph.D.                      Date  
Vice President for Development and                      6/20/22  
Alumni Relations

  
\_\_\_\_\_  
Marybeth Boger, Ph.D.                      Date  
Vice President for Student Affairs                      6-13-22  
and Dean of Students

  
\_\_\_\_\_  
Dale A. McLeod                      Date  
Vice President for Human Resources                      6/15/22

  
\_\_\_\_\_  
Simon Nynens                      Date  
Vice President and Chief Commercial                      6/15/22  
Officer

## **Appendix A: Minimum Security Standards**

**Note:** The minimum security standards will be published on the IST webpage. This section will provide a link to the webpage with the published standards.

<https://ist.njit.edu/policy-and-standards>

## Appendix B

**Table 1. Data Classification and Description**

Information Classification	Description	Examples
Restricted	Data is classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a <b>high level of risk</b> to the university or its affiliates. The users of Restricted data must follow all safeguards for Sensitive data plus additional safeguards identified for Restricted data. High levels of security safeguards must be applied to Restricted data.	<ul style="list-style-type: none"> <li>● Student Educational Records subject to the Family Educational Rights and Privacy Act (FERPA), including but not limited to transcripts</li> <li>● Social Security Number</li> <li>● Passport Number</li> <li>● Driver's License Number</li> <li>● PHI and data covered by HIPAA</li> <li>● Bank/Financial/Credit Card Account Numbers</li> <li>● University Financial Data</li> <li>● University Research Data I.e. Export Controlled data, ITAR/CUI</li> <li>● Litigation related information and privileged legal communications</li> <li>● Police Records</li> </ul>
Sensitive	Data is classified as Sensitive if the unauthorized disclosure, alteration or destruction of that data could result in a <b>moderate level of risk</b> to the university or its affiliates. By default, all institutional data that is not explicitly classified as Restricted, Internal or Public data must be treated as Sensitive data. A reasonable level of security safeguards must be applied to Sensitive data.	<ul style="list-style-type: none"> <li>● Login credentials - UCID and password</li> <li>● Non-public business communications, emails, and internal memos, and any type of documents and forms</li> <li>● Any student, personnel or alumni bio data not covered by Restricted University Intellectual Property</li> <li>● University sponsors and donors' information</li> <li>● Employee home address</li> <li>● Directory information for employees who have requested non-disclosure</li> <li>● Directory information for student who have requested non-disclosure under FERPA</li> </ul>
Internal	Data is classified as Internal if the unauthorized disclosure, alteration or destruction of that data could	<ul style="list-style-type: none"> <li>● Licensed Software</li> <li>● NJIT ID number (employee ID, student ID)</li> </ul>

	<p>result in a <b>low level of risk</b> to the university or its affiliates. Data that is shared with members of the University community or subsets of the university community. Internal data is neither classified as <b>Restricted</b> nor <b>Sensitive</b> — however, it is still protected and you must take care to safeguard it, and to prevent unauthorized access by those who are not NJIT students, faculty, or employees.</p>	<ul style="list-style-type: none"> <li>● Directory Information for student who have not requested non-disclosure under FERPA (i.e., <a href="http://directory.njit.edu">directory.njit.edu</a>, name, telephone)</li> <li>● Employee Training information</li> <li>● Web-based resources designed for non-Public University use</li> </ul>
Public	<p>Data that is readily available to the public. This data requires no confidentiality.</p>	<ul style="list-style-type: none"> <li>● UCID</li> <li>● Course Catalog</li> <li>● Employee Directory Information</li> <li>● Publicly Accessed Websites</li> <li>● Publicly Accessed Research Data (at data owner's discretion)</li> <li>● Press Releases</li> <li>● Board of Trustee Resolutions</li> </ul>