Data Classification Matrix

	Confidential	Restricted	Public
Description	Data should be classified as Confidential when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the Institution or its affiliates. Examples of Confidential data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. Data that would provide access to Confidential or Restricted data is considered Confidential (e.g., username with password). The highest level of security controls should be applied to Confidential data.	Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the Institution or its affiliates. By default, all Institutional Data that is not explicitly classified as Confidential or Public data should be treated as Restricted data. A reasonable level of security controls should be applied to Restricted data.	Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the Institution and its affiliates. Examples of Public data include press releases, course information and research publications. While little or no controls are required to protect the confidentiality of Public Data, some level of control is required to prevent unauthorized modification or destruction of Public data.
Legal/Regulatory Requirements	Law/regulation dictates that protection of data is required.	Protection of data is at the discretion of the Institution and the applicable Data Steward.	Protection of data is at the discretion of the Institution and the applicable Data Steward.
Reputational Risk	High	Medium	Low
Data Access and Control	Legal, ethical, or other constraints prevent access without specific authorization. Data is accessible only to those individuals designated with approved access and signed non-disclosure agreements; and typically on a business "need to know" basis only.	Data is accessible only to those individuals designated with approved access and signed non-disclosure agreements; and typically on a business "need to know" basis only.	No access restrictions. Data is available for public access.
Transmission	Transmission of Confidential data through any non-New York Tech network, New York Tech guest network, or any electronic messaging system (e-mail, instant messaging, text messaging) is prohibited.	Transmission of Restricted data through any non-New York Tech wired network is strongly discouraged. Transmission through any electronic messaging system (e-mail instant messaging, text messaging), is also strongly discouraged.	No other protection is required for public information; however, care should always be taken to use all Institution information appropriately.
Storage	Storage of Confidential data is prohibited on unauthorized computing/storage equipment unless approved by Information Technology Services. This includes storage in cloud based solutions such as Google Docs and Microsoft OneDrive.	Storage of Restricted data is prohibited on unauthorized computing/storage equipment unless approved by Information Technology Services. If approved, ITS approved encryption is required.	No other protection is required for public information; however, care should always be taken to use all Institution information appropriately.
Documented Backup and Recovery Procedures	Documented recovery and backup procedures are required.	Documented recovery and backup procedures are required.	Documented backup and recovery procedures are not necessary, but strongly encouraged.
Documented Data Retention Policy	Documented data retention policy is required.	Documented data retention policy is required.	Documented data retention policy is not required, but strongly encouraged.
Audit Controls	Data Stewards with responsibility for Confidential Data must periodically monitor and review their systems and procedures for potential misuse and/or unauthorized access.	Data Stewards with responsibility for Restricted Data must periodically monitor and review their systems and procedures for potential misuse and/or unauthorized access.	No audit controls are required.
Examples of Data	Data used to authenticate or authorize individuals to access electronic resources such (e.g., passwords, keys or other electronic tokens, etc.). Personally Identifiable Information (PII): Last name, first name or initial with any one or more of the following data elements: - Social Security Number (SSN) - Driver's license - State ID card - Passport number - Financial/banking account, credit card, or debit card numbers Protected Health Information (PHI)* - Health status - Healthcare treatment - Healthcare payment Student data not included in directory information** - Loan or scholarship information - Student tuition bills, payment history - Student financial services information - Class lists, enrollment information - Transcripts/grade reports - Disciplinary action - Athletics or department recruiting information * Exceptions apply ** Case law related to FERPA suggests that email containing information about a student's academic performance is not considered part of a student's "education record" unless the email is centrally maintained by the Institution (e.g., printed off and placed in the student's file). NY Tech suggests that faculty and staff be very mindful and attentive to the seriousness of the information being communicated about students as email is not a secure means of transmission.	Personal/Employee/Student Data - NYIT ID number - Salary/benefits information - Personnel records, performance reviews - Race, ethnicity, nationality, gender - Date and place of birth - Directory/contact information designated by the owner as private - ID card photographs for Institution use - Criminal background check records and credit reports Business/Financial Data - Financial transactions which do not include confidential data - Information covered by non-disclosure/confidentiality agreements - Legally privileged information - Contracts that do not contain PII or PHI - Credit reports - Records on spending, borrowing, net worth Academic/Research Information - Library transactions - Unpublished research or research detail results that are not confidential data - Private funding information - Human subject information - Course evaluations Anonymous Donor Information Last name, first name or initial (and/or name of organization) with any of the following: - Telephone/fax numbers, e-mail and employment information - Family information (spouse, partner, guardian, children, grandchildren, etc.) Management Data - Detailed annual budget information - Conflict of Interest Disclosures - Institution's investment information Systems/Log Data - Server event logs	Certain directory/contact information not designated by the owner as private. - Name - Address (campus or home) - Listed telephone numbers - Degrees, honors and awards - Most recent previous educational institution attended - Major field of study - Dates of current employment, position Specific for students: - Class year - Participation in campus activities and sports - Weight and height (athletics) - Dates of attendance - Status Business Data - Campus maps - Job postings - List of publications (published research) - Press Releases