**Data Classification Matrix**

<table>
<thead>
<tr>
<th>Description</th>
<th>Restricted</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data should be classified as Confidential when the unauthorized disclosure, alteration, or destruction of that data would 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.</td>
<td>Data should be classified as Restricted when the unauthorized disclosure, alteration, or destruction of that data would result in little or no risk to the institution and its affiliates. By default, all Institutional Data that is not explicitly classified as Confidential or Restricted data should be treated as Restricted data. A reasonable level of security controls should be applied to Restricted data.</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.
- 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.

**Transmission**

- Transmission of Confidential data through any non-New York Tech network, New York Tech internal 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, IT’s encryption tool 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 as (e.g., passwords, keys or other electronic tokens, etc.):
  - Personal/Employee/Student Data:
    - NYIT ID number
    - Social Security Number (SSN)
    - Driver’s License
    - Passport number
    - Financial/banking account, credit card, or debit card number
  - Protected Health Information (PHI)*:
    - Health status
    - Healthcare treatment
    - Healthcare payment
  - Student data not included in directory information**:
    - Name
    - Address (campus or home)
    - Telephone numbers
    - Degrees, honors and awards
    - Most recent educational institution attended
    - Dates of current employment, position
  - Business/Financial Data:
    - Financial transactions which do not include confidential data
    - Financial/banking information
    - Social Security Numbers (SSN)
    - Student’s ID number
    - Parent’s ID number
  - Academic/Research Information:
    - Library transactions
    - Academic transcripts
    - Faculty/Staff information
  - Unpublished research or research detail results that are not confidential data:
    - Manuscripts
    - Research details
  - Personal Information:
    - Personal background information
    - Personal biographical information
  - Data always applies:
    - Student’s name, date of birth, address, telephone number, social security number
  - Exceptions apply:
    - Student’s name, date of birth, address, telephone number, social security number
  - 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., printout 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.

<table>
<thead>
<tr>
<th>Data Classification Matrix</th>
<th>Restricted</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data should be classified as Confidential when the unauthorized disclosure, alteration, or destruction of that data would 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.</td>
<td>Data should be classified as Restricted when the unauthorized disclosure, alteration, or destruction of that data would result in little or no risk to the institution and its affiliates. By default, all Institutional Data that is not explicitly classified as Confidential or Restricted data should be treated as Restricted data. A reasonable level of security controls should be applied to Restricted data.</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.
- No other protection is required for public information; however, care should always be taken to use all Institution information appropriately.
- No other protection is required for public information; however, care should always be taken to use all Institution information appropriately.

**Transmission**

- Transmission of Confidential data through any non-New York Tech network, New York Tech internal 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, IT’s encryption tool 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 as (e.g., passwords, keys or other electronic tokens, etc.):
  - Personal/Employee/Student Data:
    - NYIT ID number
    - Social Security Number (SSN)
    - Driver’s License
    - Passport number
    - Financial/banking account, credit card, or debit card number
  - Protected Health Information (PHI)*:
    - Health status
    - Healthcare treatment
    - Healthcare payment
  - Student data not included in directory information**:
    - Name
    - Address (campus or home)
    - Telephone numbers
    - Degrees, honors and awards
    - Most recent educational institution attended
    - Dates of current employment, position
  - Business/Financial Data:
    - Financial transactions which do not include confidential data
    - Financial/banking information
    - Social Security Numbers (SSN)
    - Student’s ID number
    - Parent’s ID number
  - Academic/Research Information:
    - Library transactions
    - Academic transcripts
    - Faculty/Staff information
  - Unpublished research or research detail results that are not confidential data:
    - Manuscripts
    - Research details
  - Personal Information:
    - Personal background information
    - Personal biographical information
  - Data always applies:
    - Student’s name, date of birth, address, telephone number, social security number
  - Exceptions apply:
    - Student’s name, date of birth, address, telephone number, social security number
  - 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., printout 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.