SECTION 1: POLICY STATEMENT

All members of the Bucknell University community have a responsibility to protect institutional data from unauthorized access, modification, or disclosure and are expected to understand and comply with this policy.

SECTION 2: BACKGROUND, SCOPE, & AUDIENCE

Through the normal course of business, all colleges and universities come in contact with personal information, financial details, and other information which is sensitive or confidential in nature. While some data are governed by industry or governmental regulations, other types of information may not be covered by specific regulations. Even so, it is in the community’s best interest to take steps to reasonably and responsibly safeguard private information.

This policy defines the classifications of institutional data -- i.e., the categories of data that the University is responsible for safeguarding -- and the associated measures which are necessary to safeguard each classification. Institutional data commonly exists in many forms, including electronic, magnetic, optical, and traditional paper documents. Common types of electronic data include email messages, spreadsheets, word processing documents, PDF reports, as well as centrally-managed databases and file storage systems.

This policy does not apply to data whose copyright is owned by individual faculty members, staff, or students as defined by the University’s Intellectual Property policy.

This policy applies to all University faculty, staff, students, student employees, volunteers, and contractors who have access to sensitive or confidential information as defined in this document. This policy covers data that are stored, accessed, or transmitted in any and all formats, including electronic, magnetic, optical, paper, or other non-digital formats.

With the exception of those classes of data expressly protected by statute, contract, or industry regulation, the data classification examples presented below are guidelines. The data steward is ultimately responsible for the classification of data under his or her management. Classifications for particular data sets may be adjusted based on risk assessment or documented business need.

SECTION 3: DEFINITIONS

Data Steward: a senior-level employee of the University who oversees the lifecycle of one or more sets of institutional data. Data stewards are responsible for the maintenance of data elements and the authorization of their use by parties outside of their department or institution. Data steward responsibilities generally fall to managers of departments which own the data collections under consideration.
SECTION 4: DATA CLASSIFICATIONS AND DEFINITIONS

Data that are created, processed, collected, or maintained by the University is classified into the following three categories:

1. Public
2. Sensitive
3. Confidential

4.1: Public Data

Public data are institutional information that may or must be freely available to the general public. It is defined as information with no existing local, national, international, or contractual restrictions on access or usage.

Common types of public data include the following:

- Faculty, Staff, and Student directories
- Campus maps
- Course Catalogs
- Events Calendars

4.2: Sensitive Data

Sensitive data are institutional information that must be guarded due to proprietary, ethical, privacy, or business process considerations. Sensitive data must be protected from unauthorized access, modification, transmission, storage or release. This classification applies even though there may be no legal or contractual controls which require such protection. By default, most administrative data fall into this classification.

Common types of sensitive data include the following:

- Admission applications
- Educational records and information protected by the Family Educational Rights and Privacy Act (FERPA)
- Employment applications, personnel files, benefits information, salary, birth dates, and personal contact information
- Donor information: personal contact details, donation and gift amounts that are not disclosed to the public
- Privileged attorney-client communications
- Non-public University policies
- University internal memos and email, internal reports, budgets, plans, and financial information
- Non-public contracts
- Faculty, staff, and student ID numbers
- Research data that have not been intentionally released
4.3: Confidential Data

Confidential data are institutional information protected by government regulations, statutes, industry regulations, contractual obligations, or specific University policies. Administrators and data stewards may designate additional types of institutional data as confidential. Confidential data should be disclosed to individuals and business partners on a strict need-to-know basis. Disclosure to parties outside the University should be expressly authorized by the appropriate data stewards.

Common types of confidential data include:

- Data protected by the Payment Card Industry (PCI) including credit card numbers, card security codes (CVV2 codes), and authorization codes
- Data protected by the Health Insurance Portability and Accountability Act (HIPAA) including healthcare information and insurance policy numbers
- Password, password hashes, encryption keys, and cryptographic tokens used for authentication to any University information systems or for the encryption of any other confidential data
- Individuals’ unique identification details including social security, driver’s license, passport, and student/travel visa numbers
- Magnetic stripes, barcodes, or proximity (RFID, NFC, etc.) data which are encoded on identification cards or key fobs and is used for authentication, point of sale, or physical security systems.
- Financial account details including checking, investment, or retirement account numbers
- Any data which are export-controlled information under applicable laws

SECTION 5: DATA PROTECTION

Bucknell University has the following guidelines in place to protect each classification of data.

5.1: Public Data

While there are no restrictions on access to public data, such data should be properly secured to prevent their unauthorized modification, unintended use, or distribution. It should be understood that any information that is widely disseminated within the campus community is potentially available to the public at large.

The following guidelines are for information systems which are used to store and share Bucknell’s public data.

- When practical, public data should only be shared via systems over which the University maintains full administrative control, which includes the ability to remove or modify the data in question
- Information systems such as web servers which are used to share public data must be properly secured to prevent the unauthorized modification of published public data
- Interactive access to databases containing public data such as online directories or library catalogs should be properly secured using query rate limiting, CAPTCHAs, or similar technology to impede bulk downloads of entire collections of data
5.2: Sensitive Data

Sensitive data require some level of protection because its unauthorized disclosure, alteration, or destruction might cause damage to the University. The requirements for handling sensitive data are as follows.

In addition to the requirements outlined for public data, sensitive data must be:

- Protected in order to prevent loss, theft, unauthorized access and/or unauthorized disclosure
- Stored in a closed container (i.e. file cabinet, closed office, or department where electronic door access control systems are in place) in order to prevent disclosure when not in use

Furthermore, sensitive data:

- Must not be disclosed to parties outside of the University without explicit written authorization by an appropriate data steward.
- Must not be stored on any cloud-based information systems not managed or contracted by the University. *(See Section 6 for additional details about approved storage and transmission of sensitive data.)*

5.3: Confidential Data

Confidential data require a high level of protection due to the risk and magnitude of loss or harm that could result from disclosure, alteration, or destruction of the data. The requirements for the handling of confidential data are as follows.

In addition to the requirements outlined for sensitive data, confidential data must be:

- Protected with strong passwords and stored on devices which have protection and encryption measures provided by Library and IT (LIT) in order to protect against loss, theft, unauthorized access and unauthorized disclosure
- Protected by LIT-approved encryption when stored on any devices or media that are not physically tethered to the University such as mobile devices, optical or flash media, or backup tapes. *See the Mobile & Remote Device Policy for further details about mobile devices.*
- Protected by LIT-approved encryption when transmitted across public networks such as the Internet
- Protected by multi-factor authentication whenever such capabilities exist
- Accessed via an LIT-approved VPN when queried from a remote location
- Stored only on University-owned devices -- confidential data are not permitted to be stored on any personally owned devices including mobile phones, laptops, or home computers. *(See the Mobile & Remote Device Policy for more details.)*
- Must be stored only in a locked drawer; a locked room; an area where access is controlled by a guard, cipher lock, and/or card reader; or an area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other individuals not on a need-to-know basis

Section 6: Quick Reference Guide for IT Services
The following chart is meant to serve as a quick reference for IT services. If not specified below, contact Library and IT (L&IT) before using a service to store, process, or transmit sensitive or confidential data as defined by this policy.

<table>
<thead>
<tr>
<th>Category</th>
<th>Service</th>
<th>Public</th>
<th>Sensitive</th>
<th>Confidential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internally-Hosted Services</td>
<td>Shared personal folders</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Shared public folders</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Shared departmental folders (secured via group)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Voicemail</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Cloud Services</td>
<td>Institution-provided Cloud Drive</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Other personally-provisioned cloud services</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>