Bucknell UNIVERSITY

Data Classification and Management

Effective Date: February 15, 2018

Summary

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.

Background, Scope, and Audience

Through the normal course of business, employees at Bucknell University collect, maintain, transmit and/or have access to personal information, financial data, and other information which is sensitive or confidential in nature. The protection of some types of data is governed by industry or governmental regulations. While other types of information may not be covered by specific legal requirements, it is in Bucknell's best interest to take steps to reasonably and responsibly safeguard all 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, and 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 herein. This policy covers data that is 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 in this document are guidelines. Ultimate responsibility for the classification of data in the Bucknell environment is determined by the Data Steward of a particular set of data.

Data Classification

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

1. Public – Public data is institutional information that may or must be freely available to the general public. Such information has no local, national, international, or contractual restrictions on access or usage.

2. Sensitive – Sensitive data is 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 will fall into this classification.
3. Confidential – Confidential data is institutional information protected by law, 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 is only to be disclosed to individuals and business partners within the university on a strict need to know basis. Disclosure to parties outside the University must be expressly authorized by the appropriate data stewards with applicable security controls and expectations prescribed in written form.

Data Protection

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

Public Data

While there are no restriction on access to public data, such data should be properly secured to prevent unauthorized modification, unintended use, or inadvertent/improper 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 or cloud services 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, CAPTCHA's or similar technology to impede bulk downloads of entire collections of data.

Sensitive Data

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

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

- If stored in the cloud, stored only on cloud-based information systems managed or contracted by the University.
- Protected through the use of authenticated access in order to prevent loss, theft, or unauthorized access, disclosure or modification.
- In the case of printed sensitive data such as reports, stored in a secure manner (file cabinet, closed office or department where electronic door access control systems are in place) when not in use.

Confidential Data

Confidential data requires the highest level of protection due to the risk and magnitude of loss or harm that could result from disclosure, alteration, or destruction of the data. Certain types of data such as health information may have additional requirements for protection. Wherever possible, confidential information should remain in source systems and not propagated through saved files, spreadsheets, or other file formats. 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 appropriate protection and encryption measures provided by Library and IT (L&IT) in order to protect against theft, unauthorized access and unauthorized disclosure.
- Protected by L&IT-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 and Remote Device Policy for further details about mobile devices.
- Protected by L&IT-approved encryption when transmitted across public networks such as the Internet.
- Protected by multi-factor authentication whenever such capabilities exist.
- Accessed via an L&IT-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.)
- Printed material must be stored only in a locked drawer; a locked room; an area where access 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

Credit Card Data (PCI)

Information regarding credit card transaction requires specific protections which Bucknell is expected to adhere to as part of our ability to conduct credit card transactions. Credit card data

includes: full track information (swipe), credit card number, CVV or CVC, and PIN code. This data must be properly destroyed once the transaction has been completed. Any system that Bucknell uses must be PCI-DSS compliant with the implemented version of software. Questions surrounding the acceptance of processing of credit cards should be directed to the Finance Office or Information Security.

Data Type	Common Data Examples	Internally Hosted Services				Cloud Based Services	
		Personal Folder	Dept. Folder	Public Folder/Storage	Voicemail	University Provisioned	Personal
PUBLIC	Faculty, Staff, and Student Directories, Campus Maps, Course Catalogs, Events Calendars	YES	YES	YES	YES	YES	NO
SENSITIVE	Admissions Applications, Educational records and information protected by 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 no been intentionally released	YES	YES	NO	YES	YES	NO
CONFIDENTIAL	Credit card authorization codes, Healthcare information protected by the Health Insurance Portability and Accountability Act (HIPAA) and insurance policy numbers, Personally Identifiable Information (PII) including Social Security Number, Driver's License, Passport, and student/travel Visa numbers, Magnetic stripe data, barcodes, or proximity card data which is encoded on media 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	YES	YES	NO	NO	YES	NO
CREDIT CARD (PCI)	Full track card data, credit card number, card validation code or value (CVV), or PIN Code **(NOTE: Card data may only be stored /processed via systems that have received PCI-DSS certification)**	NO					

Policy Name: Data Classification Policy		*Policy ID:* IS-003
Related Policies:		
- Data Governance Policy		
Policy Owner: Chief Information Security Officer		
Policy Reviewed By:		*Next Policy Review Date:*
- General Counsel - Enterprise Systems Advisory Council - Committee on Library and Information Resources	Nov/2017 Oct/2017 Oct/2017	September 2018