Bucknell
UNIVERSITY

Information Security Policy

Effective Date: February 15, 2018

Summary

The Information Security Policy sets forth Bucknell University’s expectations in providing computing and networking facilities in the support of academic pursuits, as well as the administrative and residential needs of our students, faculty, and staff.

The Information Security Policy, in conjunction with the Acceptable Use Policy (AUP), sets the foundation for responsibilities of our constituents in protecting university resources as well as the privacy of individuals.

Scope

This policy applies to all Bucknell L&IT staff and any university faculty, staff or students responsible for management of non-IT managed systems or cloud services (including SaaS and PaaS).

Information Security Policy

Bucknell University’s Chief Information Security Officer has overall responsibility and accountability for establishing a secure IT environment.

This policy establishes general best practices associated with all systems and services in support of the university.

Privacy

While there should be no legal expectation of privacy in Bucknell provided resources, Bucknell does seek to protect the privacy interests of its constituents, while still providing the ability to provide the necessary visibility for information security to be effective in detecting and responding to various threats. In balancing the needs of privacy and information security, the University commits to:

- Wherever possible will leverage automated tools in analyzing data collection. This serves to not only focus limited personnel resources on investigating potential issues, but also to help protect individual identity
- Wherever possible will leverage non identifiable information such as IP address in investigating possible incidents
- Will only resolve individual user names or traffic information at the direction of the Chief Information Security Officer for information security related events or General Counsel for all other requests.
- Any suspicion of Illegal activities must be immediately reported to the Chief Information Security Officer or Public Safety

System Access

Need to Know – Access to information in the possession of, or under the control of Bucknell University must be provided on a need to know basis. Information must be disclosed only to individuals who have a legitimate business need for information. At the same time, workers must not withhold access to information when the owner or data steward of the information instructs that it be shared. To implement the need to know concept, Bucknell University has adopted an access request and owner approval model. When a staff or faculty member changes job duties including termination, transfer, promotion or leave of absence, his or her supervisor must immediately notify Library & Information Technology of the change. The privileges granted to all workers must be periodically reviewed (at least annually) by Information Owners and Data Stewards to ensure that only those with a current need to know presently have access.

User IDs and Passwords – To implement the need-to-know process, Bucknell University requires that each individual accessing information systems have a unique user ID and a private password. These user ID's must be employed to restrict system privileges based on job duties, project responsibilities, and other business activities. Wherever possible, the User ID and password requirement should leverage the university's existing Single Sign On solution to ensure adherence to this policy.

Password Requirements (Multi-Factor Authentication) – Systems that leverage MFA have the following password requirements:

- Password Length (minimum) – 14 characters
- Password Complexity – Password must contain at least one uppercase, one lowercase, one numeric, and one special character. The use of passphrases is encouraged.
- Password Change Frequency – Systems requiring MFA do not require regular password changes. Forced password changes will be required in the event of potential exposure through phishing or other password misuse.
- Password Re-use – Passwords may not be reused

Password Requirements (Non Multi-Factor Authentication) – Systems that do not support the use of MFA

- Password Length (minimum) – 14 characters
- Password Complexity – Password must contain at least one uppercase, one lowercase, one numeric, and one special character. The use of passphrases is encouraged.
- Password Change Frequency – Passwords must be changed every 180 days
- Password Re-use – Passwords may not be reused

Password Storage – Passwords must not be stored in readable form in batch files, automatic logon scripts, software macros, computers without appropriate access controls systems, or in other areas where unauthorized persons might discover them.

Access Monitoring

System logs should be reviewed for inappropriate access on a regular basis (at least monthly) or via automated systems capable of detecting misuse through analyzing frequent password failures, geographic anomalies, or inappropriate access attempts.

Protection of Data

Certain classes of information stored within Bucknell University systems have regulatory requirements associated with their storage and transmission. This data includes PII (Personally Identifiable Information) including certain combinations of data regarded as sensitive PII, PHI (Personal Health Information) or PCI (Payment Card Industry) information as well as information deemed sensitive or confidential that requires additional level of protection including data encryption where appropriate.

Software Systems Security

All software and services used to process Bucknell University information are subject to an Information Security review and sign off prior to their purchase or development. Information security reviews will evaluate specific risks and controls available and necessary based on the information being processed. The system owner will be responsible for the deployment of the agreed upon security controls prior to enabling the production capability of the proposed software or system.

Vulnerability Management

All individuals (including faculty, staff, or students) who have taken on or assigned the responsibility of managing any system attached to the Bucknell network or any cloud system that holds a relationship to Bucknell University or holds Bucknell University data must ensure the timely implementation of operating system and application patches to ensure the confidentiality, integrity, and availability of said systems or data. The timeliness of patches will be evaluated on the risk to the institution based on information contained in the Common Vulnerabilities and Exposures or U.S. National Vulnerability Databases, but in no instance should be in excess of 120 days behind in any patches. All systems shall be enrolled in the university vulnerability assessment and management solution.

Privileged Account Management

Accounts with privileged access to services and systems (administrative privileges) may not use the same credentials individuals use on a daily basis to access systems such as their workstation, myBucknell, or university e-mail. Privileged accounts due to their nature require stronger passwords (minimum of 20 characters) and must use MFA wherever possible. Privileged account passwords should be stored where possible in the university privileged account management (PAM) tool or if not available can be stored in a password manager.

Mandatory Reporting

All suspected policy violations, system intrusions, virus infections, and other conditions that might jeopardize Bucknell University information or information systems must be immediately reported to the Chief Information Security Officer.

Exceptions

Any exceptions to this policy must be completed in writing and include the system details, vulnerability, reason for exception, risk mitigations put in place, and remediation plan for compliance with policy. Exceptions will be reviewed by the Chief Information Security Officer or their designate on at least an annual basis for either compliance or further remediation of the exception. Depending on severity of exception and/or potential exposure of information, a senior official of the university may be required to acknowledge and accept any risk from proposed exceptions.

<table>
<tr><td colspan="2"><i>Policy Name:</i> Information Security Policy</td><td><i>Policy ID:</i> IS-002</td></tr>
<tr><td colspan="3"><i>Related Policies:</i></td></tr>
<tr><td colspan="3">- Appropriate Use Policy
- Data Classification and Management Policy</td></tr>
<tr><td colspan="3"><i>Policy Owner:</i> Chief Information Security Officer</td></tr>
<tr><td colspan="2"><i>Policy Reviewed By:</i></td><td><i>Next Policy Review Date:</i></td></tr>
<tr><td>- General Counsel</td><td>Nov/2017</td><td>September 2018</td></tr>
<tr><td>- Enterprise Systems Advisory Council</td><td>Oct/2017</td><td></td></tr>
<tr><td>- Committee on Library and Information Resources</td><td>Oct/2017</td><td></td></tr>
</table>