Information Security Policy

Effective Date:	January 14, 2026
Revised Date:	January 14, 2026
Department:	Information Technology
Administration:	Chief Information Security Officer

PURPOSE

The purpose of this policy is to protect Butler University's information and technology resources by ensuring their confidentiality, integrity, and availability. It establishes a framework of security standards, roles, and responsibilities that support compliance with federal and state regulations (including FERPA, HIPAA, and GLBA), manage risks to institutional data, and uphold the trust placed in Butler by students, faculty, staff, affiliates and partners. The policy is intended to balance strong security with usability so that academic and administrative activities can thrive in a secure environment.

POLICY STATEMENT

1. Butler University is committed to maintaining a secure information environment by implementing appropriate administrative, technical, and physical safeguards. All members of the university community must:
    a. Handle institutional data according to its classification level (e.g., public, internal, restricted, critical). Additional information regarding data classification can be found in the Data Policy.

    b. Use university IT resources responsibly and in accordance with the Acceptable Use Policy.

    c. Promptly report suspected security incidents, vulnerabilities, breaches, improper access, or technology theft/loss to IT (security@butler.edu).

2. Roles and Responsibilities
    a. Chief Information Security Officer (CISO): Oversees implementation of security policies, risk assessments, and incident response.
    b. IT Security Team: Develops and enforces security standards, manages audits, and investigates incidents.
    c. Data Stewards: Ensure proper handling of data within their functional areas.
    d. End Users: Follow security policies, complete training, and report security concerns.

3. Definitions
    a. Sensitive Information: Any private, non-public data owned or administered by Butler University regarding university business, employees, students, or other individuals associated with the university (encompassing all levels of data classification other than “Public”).
    b. Breach: Unauthorized exposure, disclosure, or loss of sensitive information.
        i. Indiana Code (IC 24-4-14) indicates breach has occurred per law whenever:
            1. Social Security number is disclosed when not encrypted and includes more than five digits
            2. -or-
            3. Individual's first and last name or first initial and last name and one or more of the following are disclosed:
                a. Driver's license number
                b. State ID card number
                c. Credit card number, or Financial account number/debit card number and security code/password, or access code.
    c. Incident: An information security incident is any attempted or actual unauthorized access, use, disclosure, modification, or destruction of information; interference with IT operations; or violation of university IT policies, including but not limited to malware infections, data breaches, phishing attacks, unauthorized system access, and denial-of-service attacks

4. Security Controls
    a. The university will implement and maintain security measures that may include:
        i. Access Controls: Role-based access to systems and data; use of multi-factor authentication (MFA).
        ii. Data Protection: Encryption of sensitive data at rest and in transit; secure storage and disposal of physical records.

        iii. Data Loss Prevention: Tools, techniques, and best practices designed to prevent sensitive information from leaving Butler's control
        iv. System Security: Regular patching, malware protection, and vulnerability scans.
        v. Network Security: Firewalls, intrusion detection/prevention systems (IDS/IPS), Network Access Control technology, and secure remote access protocols.
        vi. Incident Response: Formal procedures for detecting, reporting, and responding to security incidents.
        vii. Physical Security: Access control is in place to restrict physical access to secure locations with additional PIN-code verification required in highly sensitive areas.
    b. Network Security
        i. Information Technology will establish standards for the secure connection of university owned and personally owned computing devices to the Butler network. Access to sensitive systems may require a secure VPN or wired connection and additional authentication.
        ii. Butler employs firewall technology to protect the campus network by controlling incoming and outgoing network traffic, preventing unauthorized access, and segmenting internal resources.
            1. The default policy is "deny all, allow by exception," with rules designed to meet academic, administrative, and research needs.
            2. Firewall rule changes must be requested through Information Technology, approved by the information security team, and documented.

5. Credentials
    a. All users are responsible for protecting Butler network credentials from unauthorized use. Users may not provide system credentials, ID cards, or other personally assigned forms of authentication to any individual or third party or store system credentials in a location where they may be easily discovered by an unauthorized party.
    b. Systems containing sensitive information must include a mechanism to limit the number of unsuccessful login attempts.

6. Privileged Access
    a. All systems containing sensitive information will utilize the "principle of least privilege" with respect to the assignment of role-based access. Individuals will be provided with access only to functions necessary to fulfill job responsibilities and no more.
    b. All users of sensitive information must be accurately and individually identified.

c. Users with privileged access are responsible for complying with all applicable laws, regulations, policies, and procedures.
d. Users with privileged access must refrain from engaging in any unauthorized or inappropriate use of information and/or records, or permitting such unauthorized or inappropriate use, including accessing, viewing, altering, or otherwise engaging with sensitive information without a legitimate business reason
e. Actions undertaken by users with privileged access in Butler systems may be audited to ensure compliance.
f. Access to systems containing sensitive information will be audited by IT on an annual basis to ensure compliance.
g. Access to sensitive data by student employees is subject to additional review and restriction. Student employees may not access institutional data deemed Critical at any time.

7. System/Service Accounts
    a. A general service account is used when a program/process needs to authenticate to a system to perform functions.
    b. No automated programs or processes should run from a personal account.
    c. Service accounts must have access set to the lowest level of access needed to accomplish their job function.
    d. Administrators may not use service accounts with privileged access for unauthorized viewing, modification, copying, or destruction of system or user data.
    e. When using a service account within a process the password or access key should not be entered or stored in clear text.
    f. Service accounts should be single purpose and should not be reused for multiple systems or tasks.
    g. Periodic review of system logs is required to monitor privileged access service accounts.
    h. System administrators will be responsible for providing a list of all privileged user/service accounts with access to critical systems, applications, network devices, desktop operating systems, and file servers as well as privileged user accounts with access to user, financial and personnel data to the CISO or appointee upon request.
    i. The CISO or appointee will manage a master list of all privileged personal accounts, administrative personal accounts, local admin accounts and service accounts.

8. Storage and Disposal
    a. Electronic and physical records containing sensitive information must be adequately protected when stored, transported, or transmitted, or destroyed.

   b. Storage of sensitive information should be limited to only the data fields required to perform the university function.
   c. Sensitive information should be stored only on either Butler sanctioned system (e.g., BUfiles, Microsoft SharePoint, OneDrive) or within Butler central administrative systems (e.g., Oracle, PeopleSoft, OnBase, Slate, Advance).
   d. Sensitive information should not reside on any individual-use computer or mobile device, nor should it reside in individual-use cloud storage locations (such as Google Drive or Microsoft OneDrive.)
   e. Technology containing sensitive information must be provided to Information Technology for secure disposal (including computer equipment, USB hard drives, or other digital media).
   f. Users may access sensitive university information on personal (BYOD) devices only when it is consumed directly from the source—such as through a secure cloud application, university email, or web portal. However, sensitive data may not be downloaded to, stored on, or synced with personal devices under any circumstances.
   g. Electronic and physical records must be retained according to the University's Document Retention Schedule.

9. Incident Response
   a. Butler University is committed to responding quickly and effectively to any security incidents that may impact university data or systems.
   b. The Butler Information Technology department maintains a comprehensive Incident Response plan which is reviewed annually.
   c. All members of the university community must promptly report actual or suspected security incidents to the Information Technology Security Office by emailing security@butler.edu. Early reporting is critical for containment and damage reduction.
   d. When an incident is identified, the CISO and IT Security Team will respond to the incident according to the defined Incident Response Plan.
   e. The CISO is responsible for overseeing incident response activities, reporting updates and escalating critical incidents to the CIO and senior university leadership as necessary.

10. Risk Management
   a. Butler University is committed to proactively identifying, assessing, and mitigating information security risks to protect its data, systems, and operations. The university will employ a structured risk management process that supports informed decision-making.

b. IT, in collaboration with key stakeholders, will routinely identify potential security risks related to information systems, third-party services, and evolving threat landscapes.
c. Formal risk assessments will be conducted on a periodic basis and as needed during major system changes, acquisitions, or deployments.
d. Mitigation strategies—including administrative, technical, and physical controls—will be implemented to reduce identified risks to acceptable levels. Mitigation plans will consider the university's risk tolerance, resource availability, and legal or regulatory requirements.
e. Risk mitigation efforts will be monitored continuously to ensure effectiveness.
f. All third-party services and vendors with access to university data or systems are subject to risk review in accordance with the university's Cloud Services and Third-Party Vendor Policy.

11. Compliance

a. All users must comply with this policy and associated security standards. Violations may result in suspension of access to IT systems or further disciplinary action including dismissal.

b. All devices are subject to periodic audit to ensure compliance.

c. This policy supports compliance with applicable laws and regulations, including but not limited to:
   i. FERPA (Family Educational Rights and Privacy Act)
   ii. HIPAA (Health Insurance Portability and Accountability Act)
   iii. GLBA (Gramm-Leach-Bliley Act)
   iv. Indiana State data protection laws

SCOPE

- All university faculty, staff, students, contractors, consultants, temporary workers, and other individuals who access or use university information systems.
- All information systems, data, networks, and computing resources owned or managed by the university.
- Institutional data in all formats (electronic, paper, verbal).

EXCEPTIONS

All requests for exception must be reviewed and approved by the Chief Information Security Officer. Requests for exceptions are reviewed for validity and are not automatically approved. Requests for exception that create significant risk to the university without compensating controls will not be approved. Requests for exception must be periodically reviewed to ensure that assumptions or business conditions have not changed. Renewals are not automatically approved.

ADMINISTRATION

This policy shall be reviewed at a minimum, every three years, or when the following conditions occur:

- Security policy changes occur within IT
- University policy changes regarding the roles and responsibilities
- Federal guidelines regarding data change

RELATED POLICIES

- Acceptable Use Policy
- Data Policy
- Privacy of Personally Created Content Policy

REVISION HISTORY

- Initial version approved by University Cabinet on January 14, 2026