

UNIVERSITY POLICY



Confidential Information Policy

Responsible Office: Human Resources
Effective Date: March 24, 2025

Policy Statement

This policy outlines the University's commitment to protecting confidential information. It establishes the responsibilities of all University employees, faculty, staff, student employees, and affiliates (collectively referred to as "University Personnel") regarding handling confidential information. This policy aims to ensure compliance with applicable laws and regulations, safeguard the privacy of individuals, and protect the University's intellectual property and business interests.

Scope

This policy applies to all University Personnel who have access to or handle confidential information, regardless of their role or location. This policy extends to all forms of confidential information, regardless of format (e.g., electronic, paper, verbal).

Definitions

For purposes of this policy, the term "Confidential Information" means all of the following: *Information Protected By Law*. This includes information that is subject to specific legal or contractual obligations, such as the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), and any other applicable laws.

University Proprietary Information. This includes information disclosed to University Personnel or known to University Personnel as a consequence of the University Personnel's employment at or affiliation with the University, and not generally known outside of the University.

Information Designated as Confidential. This includes any information explicitly designated as confidential by the University.

Personally Identifiable Information. This refers to nonpublic information about employees (faculty and staff), students, and affiliates.

Examples of Confidential Information include but are not limited to – student grades; financial aid information; social security numbers; payroll and personnel records; health information; self-restricted personal data; credit card information; information relating to intellectual property; research data; passwords and other IT-related information; internal University procedures and training materials, University financial information, budget information, strategic plans, contracts, and information related to security protocols and infrastructure.

Policy

University Personnel must comply with all applicable laws, regulations and policies regarding the access, use and disclosure of Confidential Information. University Personnel may access and use Confidential Information only for legitimate University purposes. University Personnel must

protect Confidential Information from unauthorized access, use or disclosure. University Personnel must report any suspected or actual violations of this policy to their supervisor or human resources. Without limiting the generality of the foregoing, activities which are prohibited in all cases include, but are not limited to:

- Engaging in any unauthorized or inappropriate use of information and/or records, or permitting such unauthorized or inappropriate use;
- Accessing, viewing, altering, or otherwise engaging with Confidential Information without a legitimate business reason, even if system or physical access to such information is afforded to University Personnel in the course of their work assignment;
- Storing of Confidential Information in an unsecure, improper, or unapproved manner such that an unauthorized individual may obtain access to the information or record;
- Sharing of account credentials, physical keys, electronic key cards, or other means of access to Confidential Information or locations where Confidential Information is retained;
- Exhibiting or divulging contents of any record or report to any person or entity, except in the conduct of University Personnel's work assignment and/or responsibilities in accordance with Butler University policies;
- Knowingly including or causing to be included in any record or report a false, inaccurate, or misleading entry;
- Removing any physical or digital official record or report (or copy thereof) from the system or office where it is kept, except in the performance of the employee's work assignment and/or responsibilities in accordance with Butler University policies; and
- Aiding, abetting, or acting in conspiracy with any other person to violate or compromise the confidentiality of Confidential Information, or to violate this Policy.

University Personnel who violate this policy may be subject to disciplinary action consistent with the policies of Butler University, which may include termination of employment, affiliation, student disciplinary action, and possible legal action

Related Resources

- Computer Use Master Policy
- Fair, Responsible and Acceptable Computer Use Policy
- Federal HIPAA (Health Insurance Portability and Accountability Act)
- Federal FERPA (Family Educational Rights and Privacy Act) -- see Student Handbook

Policy Collaborators: Human Resources, Information Technology

Contact Information: askhr@butler.edu

Appendices: None

History/Revisions: June 2009 revision (2010 implemented)