Information Security Policy

Purpose:
Franklin Pierce University is committed to protecting confidential and sensitive information maintained by the University. The purpose of this policy is to ensure that adequate safeguards are in place to protect this information. This policy is intended to comply with other relevant University policies and with applicable laws and regulations including but not limited to FERPA and HIPAA.

Safeguarding confidential or sensitive information and information resources is essential to preserving the ability of the University to perform its mission and meet its responsibilities to students and other constituents. Failure to protect confidential or sensitive information may have financial, legal, and ethical ramifications.

Information may be deemed confidential or sensitive if its unauthorized access, modification, or loss potentially or actually causes the University to:

- be in non-compliance with legal/regulatory or contractual requirements
- suffer financial loss or damage
- adversely impact the reputation of the University or its constituents

Applicability:
This policy is applicable to all faculty, staff, students, alumni, contractors, and others who may have access to confidential or sensitive information at Franklin Pierce University. Information may include but is not limited to student financial, admission, health, or educational records and University financial data or personnel records.

Confidential or sensitive information may reside in electronic or physical form. Electronic data may reside on computing resources on campus or off-campus in the cloud. These resources may include software databases, network drives or other storage devices, personal computers, mobile devices, voice mail, other communication systems, or any peripheral device or media owned, licensed, or under contract by the University.

Responsibilities:
Each employee has responsibility for the security of information that s/he creates, uses, or maintains in the performance of his or her job function and for complying with this and other relevant policies, regulations, and laws. Various departments have primary responsibility and

authority to ensure that security requirements are met. Module managers or data stewards are responsible for developing procedures and standards to protect confidential or sensitive information in their respective area of responsibility and for communicating and advising others on appropriate use and security protocols. These departments include but are not limited to:

- Academic Affairs – student educational records
- Admissions – prospective student, student, and parent records
- Advancement Office – alumni, parent, donor records
- Business Office - financial and payroll data
- Campus Safety – student safety records
- Human Resources - personnel records
- Registrar's Office – student educational records
- Student Affairs – student and health records
- Student Financial Services – financial aid/billing/collection records
- IT – technology server and software systems

Security awareness is critical to the protection of confidential or sensitive information. The University assumes responsibility to provide training or educational resources related to security procedures, guidelines, and best practices.

Safeguarding Confidential and Sensitive Information:
In order to adequately protect confidential or sensitive information, the following minimum security requirements have been established.

Access:

- Department managers must ensure that all individuals within their department who have access to confidential or sensitive information are aware of the sensitivity of that information and understand their responsibility to protect that information appropriately.
- All users on the Franklin Pierce network must comply with relevant University policies as well as federal and state regulations and laws.
- Only users requiring access to confidential or sensitive information as part of their job function shall be granted access to that information upon approval of the appropriate manager, data steward, or senior staff member.
- Jenzabar module managers will review all user accounts and permissions for their respective module on at least an annual basis.
- All users are responsible for protecting their account passwords and for reporting any suspicious activity or security breaches immediately to their supervisor.
- Employee accounts will be disabled and passwords changed upon termination of employment or relationship with the University unless approved otherwise by senior staff (see the Account Management Policy).
- Usernames and passwords for new students must be provided in a secure manner either through postal mail or online communication.
- Passwords for all users must be a minimum of eight characters consisting of at least one upper case letter, one lower case letter, one number, and a special character (e.g.,

!#$%*&+=). Employee passwords must also be unique for the last four passwords and be changed every six months. Exceptions may be granted for employees who do not have access to change their passwords (e.g., adjunct faculty who access the network remotely) or for specific general purpose accounts.
- Employee computers must be set to automatically "time-out" after 60 minutes of inactivity and employees are strongly encouraged to log off from their computer upon leaving them unattended.

Use and Management:

- Users may not divulge, copy, loan, alter, or destroy confidential or sensitive information except as authorized within the scope of their job responsibilities.
- Confidential or sensitive information should not be stored on client laptops or computers, mobile devices, flash drives, and external or electronic devices unless it is encrypted or password protected. Confidential or sensitive information should only be stored on secure platforms or resources managed by the University.
- All University-owned servers must be protected by a firewall and have security patches and updates applied on a regular basis.
- User computers and University servers must have up-to-date and active anti-virus software.
- Rooms, offices, cabinets, closets, or other spaces where confidential or sensitive documents are stored must be locked with access limited to appropriate personnel.
- Server, network, telephone, and other rooms or closets with sensitive electronic equipment or data must be locked at all times with access limited to appropriate IT operations, Security, and Facilities staff.
- IT operations staff or designees will review relevant audit logs on a regular basis to identify potential security violations.
- The IT department will ensure appropriate data backup and recovery procedures are operational and regularly tested and that backup media is stored in a secured and environmentally controlled location.

Compliance

Any faculty, staff, student, contractor, or other person who willfully accesses, discloses, misuses, alters, destroys, or otherwise compromises confidential or sensitive information maintained by the University without authorization is subject to loss of network privileges with or without notice and/or disciplinary action up to and including termination of employment or expulsion from the University.

Franklin Pierce University may provide notice of security breaches to affected individuals and/or law enforcement agencies as deemed appropriate or required.