Stratford University

Policies and Procedures

Policy Title:	**Information Security Program**	**Approval Date**	
Policy Number		**Effective Date**	**Jan 1, 2018**
Replaces Version		**Approved By**	
Proposed by:		**Date of Submission**	Dec 10, 2017

Overview

Stratford University holds the security of student, faculty, and staff information in the highest regard and continually develops, maintains, and improves its Information Security Program to conform to the latest industry standards and best practices for storing and protecting nonpublic user and corporate data.

Purpose of Program

The Gramm-Leach-Bliley Act (Public Law 106-102) provides consumers the right to the protection of their nonpublic Personally Identifiable Information and requires financial institutions possessing such information about consumers to publish a privacy policy and implementing an Information Security Program. The Stratford University Information Security Program is in direct support of the Gramm-Leach-Bliley Act (GLBA).

Program Objectives

- Ensure protection, confidentiality, security, and integrity of student, faculty, and staff information.
- Identify and assess risks to information security, develop guidelines and procedures relevant to each information repository, and implement said procedure to protect all data.
- Evaluate, test, and refine information security processes and methodologies.

General Practices

- Periodic password resets
- Minimum password length/complexity requirements
- Multi-factor authentication
- Access POLP (Principle of Least Privilege) access model
- Physical security
- Multi-vendor end-point and systems protection (Anti-Virus/Malware)
- Regular review and improvement of Information Security Program

Information Security

As a fundamental practice, Stratford University employs the Principle of Least Privilege (POLP) for all of its Information Technology systems in which users are given the minimum level of access to information required to function in their role at the University. Furthermore, access to highly sensitive data is reserved for senior staff and is only granted on a need-to-know basis.

Password are required for access to all Stratford information data stores, systems, and services. Passwords are required to be complex, non-repetitive, and changed regularly. Access to certain privileged systems requires multi-factor authentication.

All servers have limited physical access. Stratford's core infrastructure and the servers that house our most sensitive information are located at an off-site facility with extremely limited access, employing armed guards, biometric access systems, mantraps, recorded video surveillance, etc.

All computers are protected via a combination of on premise and cloud end-point protection, virus/malware monitoring and mitigation, firewalls, and encrypted communication.

Information Systems Management

The senior Information Technology Infrastructure and Business Systems teams are tasked with ensuring that all systems are up-to-date and secure. Security patches are applied regularly to all University computers (workstations, servers, and appliances).

The ability to grant access permissions to systems and information stores is limited to a small group of IT personnel to ensure access policies are maintained. Responsibilities are segregated across systems management groups to minimize the potential for fraud and so that strict data integrity is maintained.

Access to financial systems (including Financial Aid) are specifically granted by the Controller and/or Corporate Director, Student Financial Services/Collections.

All students, faculty, and staff are provided with a unique User ID/Password for access to relevant systems. User IDs are not retired or reused, ensuring that each User ID will be unique over time. This helps prevent inadvertent access to data/resources to which one should not have access. Single Sign-On (SSO) is employed whenever possible to ensure that, once access needs to be changed/terminated, fewer touchpoints are required execute the change(s).

Protection of Personally Identifiable Information (PII)

Stratford University employs information security practices including "fair use" policies/procedures, password protected computers/servers, complex password requirements, physical security, etc. to ensure the safety of electronic and paper records. Stratford does not disclose detailed information regarding these practices to students, third parties, or the general public to safeguard the effectiveness of our procedures.

Monitoring, Testing, and Review

All services, systems, servers, and appliances are continually monitored both via technology and periodic review by senior IT staff. System access levels are tested regularly as well to ensure visibility of non-public information is maintained at the most secure levels. This program is reviewed periodically and adjusted/improved in accordance with industry best practices and the ever-changing landscape of Information Technology.