Fairleigh Dickinson University (FDU)
Policy: Safeguard Rules under the Gramm-Leach-Bliley Act

1. *Purpose:* This Policy sets the standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of information covered by applicable provisions of the Gramm-Leach-Bliley Act ("GLBA") and associated regulations. In particular, this document describes various measures being taken by FDU to (i) ensure the security and confidentiality of covered information, (ii) protect against any anticipated threats or hazards to the security of these records, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience (collectively, the "Program"). The practices described in this Policy are in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, the Family Educational Rights and Privacy Act ("FERPA").

2. *Scope of Program*: The Program applies to any record containing "nonpublic personal information" about a student or other individual who has a continuing relationship with the University, whether the record is in paper, electronic, or other form, and which is handled or maintained by or on behalf of the University ("covered information").[1] This includes any information that a student or other individual provides to FDU in connection with financial aid and tuition/fee collection efforts.

3. *Roles and Responsibilities*: Compliance and cooperation with this Policy is the responsibility of every employee at all levels within FDU. FDU's Vice President and Chief Information Officer (CIO), assisted by the Chief Information Security Officer (the "CISO"), has the overall responsibility for coordinating information security pursuant to this Policy. The CIO or CISO may designate other representatives of FDU to help oversee and coordinate particular elements of the Program. The team will work closely with other members of the Office of Information Resources and Technology (OIRT), the Data Security & Incident Response Team ("DSIRT"), the University Risk Manager, the

[1] Nonpublic personal information means: (i) personally identifiable financial information; and (ii) any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available. "Personally identifiable financial information" means any information that a consumer provides to FDU to obtain a financial product or service, any information about a consumer resulting from a transaction involving a financial product or service between FDU and that consumer, or information that FDU otherwise obtains about a consumer in connection with the provision of a financial product or service to that consumer. A "consumer" is an individual, including a student, who obtains or has obtained a financial product or service from FDU that is to be used primarily for personal, family, or household purposes, or that individual's legal representative. Examples include information an individual provides to FDU on an application for financial aid, account balance information and payment history, the fact that a student has received financial aid from FDU, and any information that FDU collects through an internet "cookie" in connection with a financial product or service.

Vice President for Human Resources, and the General Counsel, as well as relevant academic and administrative units throughout the University to implement the Program.

4. *Risk Assessment*: The CIO and CISO will help the relevant offices of FDU to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of the information; and to assess the sufficiency of the safeguards in place to controls these risks. This effort will be embodied in a risk assessment document.

The risk assessment is a written document that includes:

(i) Criteria for the evaluation and categorization of identified security risks or threats that FDU faces;

(ii) Criteria for the assessment of the confidentiality, integrity, and availability of FDU's information systems and covered information, including the adequacy of the existing controls in the context of the identified risks or threats that FDU faces; and

(iii) Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.

5. *Access Controls*: The Program includes implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to:

(i) Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of covered information; and

(ii) Limit authorized users' access only to covered information that they need to perform their duties and functions, or, in the case of third parties, to access their own information.

The Program is designed to identify and help manage safeguards for the data, personnel, devices, systems, and facilities that enable FDU to achieve its mission – efforts are prioritized in accordance with our objectives and risk strategy.

FDU has adopted authentication and access controls as needed to implement the "principle of least privilege" around accessing covered data, meaning that no user should have access greater than is necessary for legitimate FDU purposes Data owners within each applicable University unit approve and periodically review access. This includes a periodic review by the Office of Enrollment Services of all users who have access to Enrollment Services security tracks in the Colleague System and a periodic review by other administrative departments that maintain students' financial aid information regarding user access to the information.

These efforts also include employee training regarding these controls. The OIRT will coordinate with representatives in FDU's Office of Finance , Office of Financial Aid, Enrollment Services and other offices to evaluate on a regular basis the effectiveness of the University's training, procedures, and practices relating to access to and use of student records, including financial aid information as well as financial information. This evaluation will include assessing the effectiveness of the University's current policies and procedures in this area. All employees are required to train in FDU's Written Information Security Program (WISP) (training.fdu.edu), which program is incorporated by reference into this Policy.

6. *Monitoring Unauthorized Users and Use*: FDU has implemented policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, tampering with, covered information. Various specific measures are identified in Appendix 1.

These measures will include assessing the University's current policies and procedures relating to FDU's Acceptable Use Policy for Computer Usage, Confidentiality Agreement and Security Policy, FDU Procedure on Handling Data on Separating Employees, Password Policy, Policy for Acceptable Use of Email, Software Compliance & Distribution Policy, and Written Information Security Program. The CISO will also coordinate with the CIO and the OIRT to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

7. *Monitoring the Effectiveness of Safeguards:* FDU periodically conducts penetration tests and vulnerability assessments on its network and key information systems. These measures are designed to test and monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, FDU's information systems.

For those systems where continuous monitoring (or other methods to detect, on an ongoing basis, changes in information systems that may create vulnerabilities), is not practical , FDU will conduct:

> (i) Annual penetration testing on FDU's information systems identified by OIRT based on relevant identified risks under the risk assessment; and
>
> (ii) Vulnerability assessments of FDU's information systems, including systemic scans or reviews of information systems designed to identify publicly known security vulnerabilities in FDU's information systems based on the risk assessment, at least every six months; and whenever there are material changes to FDU's operations or business arrangements; and whenever there are circumstances that OIRT knows (or has reason to know) may have a material impact on FDU's information security program.

8. *Detecting, Preventing and Responding to Attacks*: The OIRT and University Risk Manager will on a regular basis evaluate procedures for and methods of detecting, preventing, and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. The FDU Data Security Incident & Response Team implements all aspects of, oversees other Departments' adherence to, and documents all incident response activities. Upon determination by the CISO and General Counsel that a Security Incident triggers breach notification laws, the University will report the breach to relevant federal or state regulatory authorities by their designated methods; and, where applicable, the U.S. Department of Education, including details about date of breach (suspected or known); impact of breach (e.g. number of records); method of breach (e.g. hack, accidental disclosure); information security program point of contact – email and phone details; remediation status (e.g. complete, in process); and next steps (as needed).

These measures will be documented in a comprehensive incident response plan that addresses:

(i) The goals of the incident response plan;

(ii) The internal processes for responding to a security event;

(iii) The definition of clear roles, responsibilities, and levels of decision-making authority;

(iv) External and internal communications and information sharing;

(v) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

(vi) Documentation and reporting regarding security events and related incident response activities; and

(vii) The evaluation and revision as necessary of the incident response plan following a security event.

9. *Overseeing In-House Developed Applications and External Service Providers*: The OIRT leadership working in collaboration with the CISO will help ensure that software applications and solutions developed in-house by FDU, including modifications to third-party programs, meet the safeguard standards of this Policy. The CIO, CISO and other appropriate OIRT leaders will also coordinate with FDU's contract review teams to raise awareness of, and to institute methods for, selecting and retaining only those service providers that can maintain appropriate safeguards for nonpublic financial information of students and other third parties to which they will have access. In addition, the CIO and CISO will work with the General Counsel and the University Risk

Manager to develop and incorporate standard, contractual protections applicable to third party service providers, which will require the providers to implement and maintain appropriate safeguards.

Utilizing a variety of automated risk assessment tools such as Bitsight, OIRT periodically assesses FDU's service providers on the risk they present and the continued adequacy of their safeguards.

10. *Encryption:* FDU adopts methods to protect by encryption covered information held or transmitted by the University by encrypting both in transit over external networks and at rest. To the extent that encryption of covered information, either in transit over external networks or at rest, is infeasible, FDU secures the covered information using effective alternative compensating controls reviewed and approved by the CISO.

11. *Multifactor authentication*: FDU has implemented multi-factor authentication for any individual accessing the University's information systems, except where the CISO has approved in writing the use of reasonably equivalent or more secure access controls.

Multi-factor authentication is defined as authentication through verification of at least two of the following types of authentication factors:

(1) Knowledge factors, such as a password;
(2) Possession factors, such as a token; or
(3) Inherence factors, such as biometric characteristics.

12. *Data Retention and Disposal Controls*: FDU has in place procedures for the secure disposal of covered information in any format, consistent with the University's operations and other legitimate business purposes, except where required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained. Where information is not needed to be retained, the University will take reasonable measures to include processes for disposal of covered information no later than two years after the last date the information is used for legitimate University purposes. The Program includes periodic review of our data retention policy to minimize the unnecessary retention of data.

13. *Adjustments to Program*: Risk assessment activities will be periodically performed to reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and to reassess the sufficiency of any safeguards in place to control these risks. The CISO is responsible for evaluating and recommending adjustments to the program based on the undertaken risk identification and assessment activities, as well as any material changes to FDU's operations or other circumstances that may have a material impact on the Program.

14. *Reports to the Board*. The Vice President of OIRT will submit written reports to the Board of Trustees at least once each calendar year. The report will include the following information:

(1) The overall status of the Program and FDU's compliance with the safeguard requirements under the GLBA;

(2) Material matters related to the Program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.

The CIO may approve deviations to the processes set forth in this Policy to meet changing conditions at the University, so long as such deviations are designed to achieve the safeguard goals set forth in this Policy and do not violate the GLBA and other applicable laws.

Appendix 1
Certain Additional Specific Safeguards

Periodically (generally at least once each year), leaders from applicable University departments and units are surveyed regarding their processes for safeguarding covered information, using a standard template. Results are compiled and conveyed to the CIO for review and follow-up, including adopting and incorporating results in the University-wide Risk Assessment.

The CIO will determine which departments and units should receive the assessment survey, based on their handling of covered information. Currently, the units are: OIRT, Office of Enrollment Services, Credits and Collections, Admissions, International Admissions, Financial Aid, Veteran Services, Accounts Payable, Management Information Systems, Conference & Summer Programs, School of Pharmacy, and the Controller's Office.

The standard assessment template is as follows.

(a) Designate an employee or employees to coordinate the unit's information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

- Unauthorized disclosure of sensitive information by employees through intentional or unintentional methods.
- Unauthorized access, disclosure, misuse, alteration or destruction of information on hosts.
- Detection and prevention of attacks on the systems.
- Unsecured transmission of data.
- Physical security of computer systems, network equipment, backups and paper materials.
- Managing data integrity and system failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

1) Unauthorized disclosure of sensitive information by employees through intentional or unintentional methods:

2) Unauthorized access, disclosure, misuse, alteration or destruction of information on hosts:

3) Detection and prevention of attacks on the systems:

4) Unsecured transmission of data:

5) Physical security of computer systems, network equipment, backups and paper materials:

6) Managing data integrity and system failures:

(d) Oversee service providers, by: (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) Requiring FDU's service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust FDU's information security program in light of the results of the testing and monitoring required by this Policy ; any material changes to FDU's operations or business arrangements; or any other circumstances that are known or have reason to be known as having a material impact on FDU's information security program.

The following is an example of a completed assessment survey, from OIRT:

Gramm Leach Bliley Security Program

Office of Information Resources Technology

Standards for Safeguarding Customer Information

(a) Designate an employee or employees to assist the CIO in the coordination of the Program.

In addition to the CISO, the Director of Systems and the Director of Networking are the designated employees for the Office of Information Resources Technology

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

- Unauthorized disclosure of sensitive information by employees through intentional or unintentional methods.
- Unauthorized access, disclosure, misuse, alteration or destruction of information on hosts.
- Detection and prevention of attacks on the systems.
- Unsecured transmission of data.
- Physical security of computer systems, network equipment, backups and paper materials.
- Managing data integrity and system failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

1) Unauthorized disclosure of sensitive information by employees through intentional or unintentional methods:

   - Employees go through mandatory Written Information Security Program (WISP) Training
   - Prior to any IT requests, User Information Is checked against WISP to ensure they are current with training

- Employees are provided training and are closely observed by managers before being given access to sensitive information. Training includes password policy and management, physical security of cabinets, storage, and equipment rooms, and recognizing fraudulent attempts to obtain sensitive information.
    - Policy, social engineering, keystrokes loggers, etc.
- All employees must sign and accept the University's "Acceptable Use Policy" and the "Confidentiality Agreement" if applicable.
- Requests for sensitive information are directed to individuals with proper training and authority to review the request.
- Potential employees are subjected to a background check before being hired by the University.
- Updated IT Informational website that includes documentation of all policies and procedures specific to securing data.
- Use of Data Loss Prevention tool to proactively monitor and correct non-compliance issues
- Access to information is granted only to the extent required for the employee to perform their job functions.

2) Unauthorized access, disclosure, misuse, alteration or destruction of information on hosts:

- Passwords are required for access to any system with sensitive information.
- Strong password policies are in place where possible.
- Multi-factor authentication to access sensitive systems for all faculty, adjuncts, staff and students.
- Multi-factor authentication for all admin accounts.
- Auditing systems (e.g. Change Management Process, Netwrix, Microsoft ATP) are used to track and report on changes to critical files.
- Notifications of employee terminations are received prior to or on date of termination. Immediate notification is received when circumstances warrant instant suspension of access to systems.

3) Detection and prevention of attacks on the systems:

- Auditing systems (e.g., Netwrix) are used to detect attempts to breach systems or alter system configurations.
- System logs are reviewed daily for evidence of attacks.
- Policies are in place to regularly apply patches to systems.
- A firewall is in place for perimeter protection.
- Obsolete systems are being replaced by newer systems that are better supported by hardware and software vendors. Most systems include host-based firewalls.
- The wired portion of the university network is entirely switched to minimize the possibility of packet sniffing and other similar attacks.
- WPA2 Enterprise is deployed and available for wireless accessible locations.
- Endpoint protection software is in place, which automatically updates servers & clients.

4) Unsecured transmission of data:

- Connections to all systems are using modern cryptographic techniques.
- University standard practice is to use HTTPS for web services; all publicly accessible web traffic is proxied through load balancers.
- SFTP is used to transmit data to various vendors securely.
- EFax services deployed, ensuring fax transmission are encrypted both in transit and at rest.
- Virtru software for encrypted email communication of sensitive and Personally Identifiable Information
- 7-Zip is used to encrypt files being sent to and from vendors.

5) Physical security of computer systems, network equipment, backups and paper materials:

- All computer systems and core network equipment are physically secured in locked rooms or cabinets.
- Essential services are monitored for availability and alerts are sent when a system or service becomes unavailable.
- Printed material with personal information is shredded when no longer needed.
- The main datacenters and several ancillary MDF's have heat and humidity detection systems as well as a fire suppression system.
- Alarms with motion detectors are in place in all data centers. The university department of Public Safety monitors the alarms.
- Security cameras are set and on 24 hour recording on both main data centers
- A card access system controls access to the data centers and IT administrative offices.

6) Managing data integrity and system failures:

- Daily backups of host systems are performed.
- Network hardware configurations are backed up weekly.
- Out of band capabilities exist to support network management and large-scale outages.
- Continual off-site backup of all FDU owned workstations.
- Mirroring of networked file services across campuses is occurring.
- UPS systems provide backup power to central data centers.
- Extending backup capabilities to include off-site backup of all University systems
- A backup generator is in place for the main data centers.
- A disaster recovery plan has been developed.

(d) Oversee service providers, by: (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) Requiring FDU's service providers by contract to implement and maintain such safeguards.

Contracts require appropriate safeguarding measures be taken by the vendor. Third Party Assessment evaluation using Industry best practice tools prior to executing contracts.

(e) Evaluate and adjust FDU's information security program in light of the results of the testing and monitoring required by this Policy ; any material changes to FDU's operations or business arrangements; or any other circumstances that are known or have reason to be known as having a material impact on FDU's information security program.

OIRT continually performs extensive reviews of applicable written policies and has a continuous program in place to review applicable policies and procedures.

OIRT periodically (generally annually) performs an eMail Phishing test to all full-time faculty and staff. FDU uses a third party as the tool for performing the test. Individuals who fail the Phishing test are required to complete remedial training with a passing score. Supervisors are made aware of those who fail the test and are encouraged to speak with their employees.

OIRT conducts comprehensive vulnerability assessments aligned to the NIST Risk Management Framework (RMF) that included external vulnerability scanning, penetration testing, netflow analysis of our IP ranges, review of IT and cybersecurity-specific and FDU-wide documentation, and dark web footprinting.

OIRT takes action to increase the cadence of monitoring and reacting to server, desktop and mobile device alerts, ensure compliance of website configurations and deploy security measures to ensure security of email system and reduce spoofing of emails.