Subject: Safeguarding Nonpublic Customer Information

1. Purpose

In order to continue to protect nonpublic personal financial information and to comply with new federal regulations mandated by the Gramm-Leach-Bliley Act (the Act), the university must establish and maintain a comprehensive information security program or policy. This policy describes the University's plan to implement the Safeguarding Standards promulgated by the Federal Trade Commission (FTC) in 16 CFR Part 314 and to meet the following objectives:

1. Ensure the security and confidentiality of customer nonpublic personal financial information records;
2. Protect against any anticipated threats or hazards to the security or integrity of such records; and
3. Protect against the unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to customers.

This policy provides documentation to instill confidence in University customers that the University is taking adequate steps to protect their nonpublic personal financial information and to minimize loss in the event of a security breach. This policy incorporates by reference the University's policies and procedures and is in addition to any University policies or procedures that may be required pursuant to other federal and state laws and regulations such as the Family Educational Rights and Privacy Act of 1974 (FERPA).

2. Policy

2.1 Policy Statement

It shall be the policy of Virginia Tech to manage nonpublic personal financial information collected from students, parents, and other third parties as confidential records. Virginia Tech has developed appropriate procedures to protect such customer financial information against reasonable threats and hazards and unauthorized access or use of such records that could result in substantial harm or inconvenience to customers. Related university policies include Policy 7100, "Administrative Data Management and Access Policy" and Policy 7000, "Acceptable Use of Computer and Communication Systems."

2.2 Responsible Position

The University Bursar is the Program Officer responsible for overseeing the implementation of the program. The Program Officer has designated the Information Technology Security Officer responsibility for ensuring the overall security of electronic systems and infrastructure for the university, including the risk assessment, security awareness, data security, threat detection, and monitoring and controlling systems activities. The Program Officer may designate other representatives of the University to oversee and coordinate additional elements of the program. Any questions regarding the implementation of the plan or the interpretation of this document should be directed to the Program Officer.

2.3 No Third-Party Rights

While this policy is intended to promote the security of information, it does not create any consumer, customer, or other third-party rights or remedies, or establish or increase any standards of care that would otherwise not be applicable.

3. Procedures

The procedures in this policy are consistent with the requirements provided in the Federal Register (16 CFR Part 314) detailing the FTC's Final Rule on the Standards for Safeguarding Customer Information and with the guidance received from the National Association of College and University Business Officers. Since the university participates in financial activities described in the Bank Holding Company Act of 1956, such as making Federal Perkins Loans and collection agency activities, the FTC considers it a financial institution for the purposes of the Act. The university is deemed to be in compliance with the privacy provisions of the Act because it complies with the requirements of FERPA.

The types of financial activities covered by the Act are typically performed by the *Office of Scholarships and Financial Aid* and the *Office of the University Bursar* but may not be limited to those departments.

3.1 Risk Analysis Process

In accordance with the Act, the Office of Scholarships and Financial Aid, the Office of the University Bursar and any other department that collect nonpublic personal financial information as described in the Act, should evaluate and update the risk assessment and related information safeguards in light of testing and monitoring results, material changes to the operations, or any other known circumstance that may have a material impact on the security of nonpublic personal financial information. Minimally, these departments must perform a risk assessment process annually.

In addition to the requirements of this Act, good business practices would include periodic assessment of the business risks faced by the departments. All university departments are strongly encouraged to complete a business impact analysis/risk assessment at least once every three (3) years (http://www.security.vt.edu/). This process provides individual units within the University information as to any potential risks and what possible safeguards are needed.

3.2 Securing Information

Departments will assess the safeguards they have in place to protect not only nonpublic personal financial customer information, but also all confidential University data. Specific safeguarding practices that departments must assess, and if necessary, implement and include in employee training, include:

1. Maintaining physical security by locking rooms and file cabinets where customer and sensitive information is stored or electronic storage is housed. Procedures should include ensuring that windows and doors are locked when areas are unoccupied and restricting access to areas where sensitive data exists.

2. Maintaining adequate key control and limiting access to sensitive areas to those individuals with appropriate clearance that require access to the area to carry out their assigned job duties.
3. Using authentication processes (such as secure passwords) and granting access privileges only to authorized personnel with legitimate business need to authorize and enforce a user's access to and actions towards specified resources.
4. Using firewalls and encrypting information when feasible.
5. Referring calls and mail requesting customer information to those individuals who have been trained in safeguarding information.
6. Shredding and erasing customer information when no longer needed in accordance with the Virginia Public Records Act and University Policy 2000, "Management of University Records."
7. Encouraging employees to report suspicious activity to supervisors and law enforcement authorities in accordance with University Policy 1040, "Reporting Suspected Fraudulent Acts."
8. Ensuring that agreements with third-party contractors who have access to nonpublic personal financial information collected by the university contain safeguarding provisions and monitoring those agreements to oversee compliance with the privacy and safeguarding provisions of the Act.
9. Ensuring that electronic hardware, electronic operating systems, software upgrades and other electronic means of storing and manipulating data are installed and configured to maintain adequate security of customer nonpublic personal financial information.

3.3 Training

Departments, such as the *Office of Scholarships and Financial Aid* and the *Office of the University Bursar* who collect nonpublic personal financial information covered by the Act, should ensure that all new and existing employees who are involved in activities covered under the Act receive safeguarding training.

Training will, at a minimum, encompass the nine "Securing Information" items listed above in 3.2. The program officer will establish a training program and designate person(s) that will conduct the training sessions. The Information Technology (IT) Security Office offers training related to security awareness and the University Registrar offers training related to privacy and FERPA compliance.

3.4 Monitoring and Detection

Department heads and responsible departmental personnel must continually assess the vulnerabilities of their electronic as well as paper-based systems. The IT Security Office and the Internal Audit and Management Services department are available to assist in assessing the efficacy of the existing safeguards and to propose improvements if needed.

3.5 Managing System Failures

The University takes every precaution to secure and protect university systems and data. Nevertheless, immediate steps should be taken to correct any security breach. Anyone who has reason to suspect a deliberate or significant breach of established security policy or procedure should promptly report it to the appropriate Dean, Director, or Department Head. The University Police and the IT Security Office should be notified as appropriate. Affected customers may also need to be notified after the department consults with the appropriate areas within the University. Examples of significant failures would include a successful hacking effort, a burglary, or impersonations leading to the defrauding of customers.

3.6 Notification to Customers

The Program Officer shall also notify the University Registrar of Virginia Tech's adherence to this program so that a compliance notification may be furnished to all students at the same time the University Registrar makes official notice of compliance with the Family Educational Rights and Privacy Act (FERPA).

4. Definitions

CUSTOMER describes students, parents, or other third parties who have disclosed nonpublic personal financial information when applying for and/or obtaining a financial service or product from Virginia Tech.

NONPUBLIC PERSONAL FINANCIAL INFORMATION includes any paper or electronic record containing nonpublic personal financial information provided by students or others in order to obtain a financial product or service from the University. Such records include loan applications, bank and credit card numbers, account histories, Social Security numbers, income tax returns, credit reports and other related customer information.

5. References

The following policies and guidelines supplement and help to create a comprehensive information security plan. Referral and adherence to these documents is imperative to overall protection of customer information. The following policies and laws are incorporated by reference into the plan:

- Policy 1040, "Reporting Suspected Fraudulent Acts."
- Policy 2000, "Management of University Records."
- Policy 7100, "Administrative Data Management and Access Policy."
- Policy 7000, "Acceptable Use of Computer and Communication Systems."
- Family Educational Rights and Privacy Act of 1974

6. Approval and Revisions

Approved May 15, 2004 by the Vice President for Budget and Financial Management, M. Dwight Shelton, Jr.

September 7, 2006: Technical revisions – policy renumbered to Information Technology Policy 7025 from former General University Policy 2025; references updated.