Safeguarding Nonpublic Customer Information

No. 7025

Policy Effective Date:
5/12/2004

Last Revision Date:
10/31/2023

Policy Owner:
Amy S. Sebring

Policy Author:
(Contact Person)
Stacy King
Lauren Lawson
Callan Bartel

Affected Parties:
Undergraduate
Graduate
Faculty
Staff
Other

1.0 Purpose
2.0 Policy
3.0 Procedures
4.0 Definitions
5.0 References
6.0 Approval and Revisions

1.0 Purpose

The purpose of this policy is to describe the university's plan to safeguard the nonpublic financial and personal customer information, whether in paper, electronic, or other form, of a consumer that is obtained or provided to the university in connection with the university providing a financial product or financial service to the consumer. In compliance with applicable regulations and laws, the university's objectives are to:

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.
3. Protect against the unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to customers.
4. Minimize loss in the event of a security breach.

2.0 Policy

The Information Technology Security Office, with support of the University Bursar, is responsible for facilitating compliance with the Gramm-Leach-Bliley Act (GLBA) and Standards for Safeguarding Customer Information (16 CFR, Part 314) through developing, implementing, and monitoring policies and procedures that include specific requirements regarding the privacy of customer financial information. Since the university participates in financial activities described in the Bank Holding Company Act of 1956, such as originating federal Direct Loans, it is the policy of the university to comply with GLBA.

The Code of Virginia § 2.2-38 (Government Data Collection and Dissemination Practices Act) mandates that Commonwealth of Virginia agencies safeguard the collection of personal information.

Virginia Tech manages the collection of nonpublic personal financial information from students, parents, research subjects, employees, and other third parties as confidential records. The following policies and procedures protect personal information against reasonable threats and hazards and unauthorized access or use of such records that could result in substantial harm or inconvenience:

- Policy 1060, Policy on Social Security Numbers;
- Policy 3610, Accepting and Handling Payment Card Transactions;
- Policy 7000, Acceptable Use and Administration of Computer and Communication Systems;
- Policy 7010, Policy for Securing Technology Resources and Services;
- Policy 7100, Administrative Data Management and Access Policy;
- Virginia Tech Risk Classification Standard; and
- Standard for High Risk Digital Data Protection.

2.1 Roles and Responsibilities

The Information Technology Security Officer is the designated Qualified Individual responsible for overseeing, implementing and enforcing the university's information security program, including Safeguarding Customer Information in compliance with 16 CFR Part 314. The Information Technology Security Officer has responsibility for ensuring university security of all electronic systems and infrastructure by:

- Periodically assessing risk to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of nonpublic personal financial 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;
- Designing, implementing, and safeguarding identified technical and physical controls;
- Testing the effectiveness of the safeguards' key controls, systems, and procedures to include detecting actual and attempted attacks on, or intrusions into information systems;
- Implementing policies and procedures to ensure personnel enact the university's program to safeguard customer information; and
- Overseeing service provider practices for managing nonpublic personal financial information.

The Qualified Individual may designate personnel of the university to coordinate elements of the program or meet the requirements using a service provider or affiliate under the Qualified Individual's direction. Any questions regarding the implementation of the plan or the interpretation of this document should be directed to the Qualified Individual.

At least annually, the Qualified Individual will report to the Board of Visitors information pertaining to the overall assessment of compliance for GLBA and specific topics related to the information security program.

2.2 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.

3.0 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. The types of financial products or services covered by GLBA are typically performed by the Office of University Scholarships and Financial Aid and the Bursar's Office but may not be limited to those departments.

3.1 Risk Analysis Process

In accordance with GLBA, the Office of University Scholarships and Financial Aid, the Bursar's Office and any other departments that collect nonpublic personal financial information from a customer seeking to obtain a financial product or service as described in GLBA, must evaluate and update the risk assessment and related information safeguards. This should be done 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 and document a risk assessment and an inventory of data and systems annually.

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 protected 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 in accordance with Policy 5620, Access Control: Key Control Policy, 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 two-factor authentication) 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. This includes regularly auditing for and removing access of users who no longer need it.
4. Using firewalls and encrypting information in accordance with current IT standards as posted on it.vt.edu.
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 Policy 2000, Management of University Records.
7. Encouraging employees to report suspicious activity to supervisors and law enforcement authorities in accordance with Policy 1040, Reporting and Investigating Suspected Fraud, Waste, and Abuse.
8. Ensuring that agreements with third-party contractors who have access to nonpublic personal financial information collected by or on behalf of the university contain safeguarding provisions and periodically assessing those service providers based on the risk they present and the continued adequacy of their safeguards.
9. Ensuring that electronic hardware, electronic operating systems, software upgrades and other physical and virtual electronic means of storing and manipulating data are installed and configured to maintain adequate security of customer nonpublic personal financial information as required by Policy 7010, Policy for Securing Technology Resources and Services, and Division of Information Technology standards and policies found on the it.vt.edu resources tab.

3.3 Training

Departments, such as the Office of Scholarships and Financial Aid and the Bursar 's Office, who collect nonpublic personal financial information covered by GLBA, must ensure employees who are involved in activities covered under GLBA receive safeguarding training upon hire and at least annually.

Training will, at a minimum, encompass the nine "Securing Information" items listed above in 3.2. The Information Technology (IT) Security Office offers training related to security awareness and IT risk assessments, the University Registrar offers training related to privacy and Family Educational Rights and Privacy Act (FERPA). compliance, and the Bursar's Office offers specific GLBA training as needed.

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 Office of Audit, Risk, and Compliance are available to assist in assessing the efficacy of the existing safeguards and to propose improvements if needed.

3.5 Managing Safeguarding Failures or Responding to Possible Data Exposure

The university takes every precaution to secure and protect university systems and data. Nevertheless, immediate steps must be taken to correct any security breach or exposure of sensitive data. In accordance with Virginia Tech Dealing with Data Exposures document, anyone who has reason to suspect a breach of established security policy or procedure should promptly report it to the appropriate Dean, Director, or Department Head. The University Legal Counsel 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 include a successful hacking effort, a burglary, or impersonations leading to the defrauding of customers.

3.6 Notification to Customers

The Qualified Individual or their designee 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 FERPA.

4.0 Definitions

CUSTOMER describes students, parents, research subjects, employees, and other third parties who have disclosed nonpublic personal financial information when applying for and/or obtaining a financial service or product from Virginia Tech. This policy applies to all academic and operational departments and offices at all university locations, owned and leased. The policies and procedures provided herein apply to all university faculty, staff, students, visitors, and contractors.

NONPUBLIC PERSONAL FINANCIAL INFORMATION includes any paper or electronic record containing nonpublic personal financial information provided by students, parents, customers, or others to obtain a financial product or service from the university. Such records include but are not limited to loan applications, account histories, Social Security numbers, income tax returns, credit reports, and other related customer information.

5.0 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 this policy:

Gramm-Leach-Bliley Act
https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf

Standards for Safeguarding Customer Information, 16 CFR, Part 314
https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

Bank Holding Company Act of 1956
https://www.govinfo.gov/content/pkg/COMPS-252/pdf/COMPS-252.pdf

Code of Virginia § 2.2-38 (Government Data Collection and Dissemination Practices Act)
https://law.lis.virginia.gov/vacode/title2.2/chapter38/section2.2-3800/

Policy 1060, Policy on Social Security Numbers
https://www.policies.vt.edu/1060.pdf

Policy 3610, Accepting and Handling Payment Card Transactions
https://www.policies.vt.edu/3610.pdf

Policy 7000, Acceptable Use and Administration of Computer and Communication Systems
https://www.policies.vt.edu/7000.pdf

Policy 7010, Securing Technology Resources and Services
https://policies.vt.edu/assets/7010.pdf

Policy 7100, Administrative Data Management and Access Policy
https://www.policies.vt.edu/7100.pdf

Virginia Tech Risk Classifications
https://it.vt.edu/content/dam/it_vt_edu/policies/Virginia-Tech-Risk-Classifications.pdf

Standard for High Risk Digital Data Protection
https://it.vt.edu/content/dam/it_vt_edu/policies/Standard-for-High-Risk-Digital-Data-Protection.pdf

Policy 5620, Access Control: Key Control Policy
https://policies.vt.edu/assets/5620.pdf

Policy 2000, Management of University Records
https://www.policies.vt.edu/2000.pdf

Policy 1040, Reporting and Investigating Suspected Fraud, Waste, and Abuse
https://www.policies.vt.edu/1040.pdf

Family Educational Rights and Privacy Act
https://studentprivacy.ed.gov/ferpa

Virginia Tech's IT Risk Assessment/ Business Impact Analysis Process
https://security.vt.edu/policies-and-compliance/it_risk_assessments

Virginia Tech's Dealing with Data Exposures
https://security.vt.edu/incident/data-exposures

6.0 Approval and Revisions

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

- Revision 1
  September 7, 2006: Technical revisions – policy renumbered to Information Technology Policy 7025 from former General University Policy 2025; references updated.

- Revision 2
  - Updates to verbiage and references.
  - Adds stipulation that proposed changes to the policy must be reviewed by the Vice President for Finance and the Vice President for Information Technology and Chief Information Officer.

  Approved January 8, 2020

- Revision 3
  - Updates to verbiage for compliance with Safeguards Rule changes.
  - Designates the Information Technology Security Officer as the Qualified Individual and adds requirement for annual Board of Visitors reporting.

  Approved October 31, 2023 by the Executive Vice President and Chief Operating Officer, Amy S. Sebring.