FTC SAFEGUARDS RULE

Gramm-Leach-Bliley Act

Effective 5/23/2003

Introduction

- The purpose of the FTC Safeguards Rule is to:
  - Ensure the security and confidentiality of customer information.
    - Customer information is defined as any record containing nonpublic personal information such as a social security number, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of VCU or its affiliates.
  - Protect against any anticipated threats or hazards to the security or integrity of such records.
  - Protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.
- This rule is governed by the Federal Trade Commission and is required by the Gramm-Leach-Bliley Act that was signed into law on November 12, 1999. Go to https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act for more information on the Gramm-Leach-Bliley Act.

Standards for Safeguarding Customer Information

- The goal of Virginia Commonwealth University is to eliminate unacceptable risks in order to safeguard customer information and protect the confidentiality and privacy rights of its customers.

Protected Customer Information

- The privacy rule limits the use and disclosure of customer information. View the Family Educational Rights and Privacy Act (FERPA) at this website: http://rar.vcu.edu/records/family-educational-rights-and-privacy-act/
- "Use" refers to what is done with the protected information, such as nonpublic information, within VCU.
- "Disclosure" refers to what is given out to an external entity for use outside of VCU.
- Covered Entities:
  - Non directory information such as social security number, grades, schedules, GPAs, bank account numbers, and academic standing.

Practical Tips for Safeguarding Customer Information

- Do not leave confidential data unattended or visible by others.
- Shred and never recycle documents containing confidential customer information such as a social security number.
- Secure all daily work in locked file cabinets or drawers.
- Protect secured areas – lock all doors, and never loan your key.
- Talk quietly when discussing confidential or private information with a customer.
  - Avoid the use of names or other identifying information whenever possible.
- Sensitive information should not be sent to remote printers or photocopiers where access is uncontrolled. Nor should it be faxed where the physical security of the receiver is unknown.
  - Include a confidential statement on your fax transmittal sheet that information sent to the incorrect destination be destroyed, and requesting notification to the sender of such errors.
  - Do not dispose of documents containing nonpublic information in wastebaskets, or recycling bins; instead, shred or otherwise destroy before discarding.
- Sensitive information should never be left on voicemail, or answering machines.
- Avoid using nonpublic information via e-mail.
- Use password-activated screensavers.

What This Means

- VCU should safeguard customers information by adhering to the following policies and guidelines:
  - Federal Educational Rights and Privacy Act (FERPA) - https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
  - State and University policies on Records Retention and Disposition - https://ts.vcu.edu/askit/policies-and-publications/records-management/
  - University Information Technology Policies and Guidelines - https://ts.vcu.edu/about-us/information-security/it-policies-standards-baselines-and-guidelines/
  - University Financial Policies - http://www.controller.vcu.edu/finpolicies/policy.htm
  - State of Virginia Information Technology Policies and Guidelines - http://www.vita.virginia.gov/library/default.aspx?id=537
  - State and University Human Resources Policies and Guidelines - http://www.hr.vcu.edu/policies/

Comments/Questions

Please forward any comments or questions to the Safeguard Coordinator, Bernard Hamm, at bchamm2@vcu.edu, or Box 842520.