Effective Date: **May 1, 2003**

POLICY

INFORMATION MANAGEMENT, PRIVACY AND SECURITY

Safeguarding Information – Gramm-Leach-Bliley Act (GLBA)

RESPONSIBLE OFFICE

Office of the Controller

Statement of Purpose

The Gramm-Leach-Bliley Act requires that the University implement a Safeguarding Program to (1) insure the security and confidentiality of certain customer information, such as student loan-related information, (2) protect against any anticipated threats to the integrity of such information and (3) protect against unwarranted, unlawful and/or unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. The Gramm-Leach-Bliley Act covers the securing and safeguarding of data. Its requirements are additional to those of the Family Educational Rights and Privacy Act (FERPA).

The Fair Debt Collection Practices Act (FDPCA) governs the collection activity of the Boston University Collection Department and also works in conjunction with the Gramm-Leach-Bliley Act.

Definitions

As used in the Gramm-Leach-Bliley Act, “customers” include those to whom the University provides financial services of any kind. For the purposes of this Safeguarding Program, “customer information” is defined as any record containing non-public, personally identifiable financial information regarding any of the University’s customers, whether such records are maintained on paper, electronically or by any other means.

Applicability

This Safeguarding Program applies to all Boston University departments with access to student loan data or other customer information regardless of the purpose or frequency of use and applies to the gathering, storing, processing, transmitting and disposing of customer information. This Program also applies to outside service providers, such as loan servicing agents and collection agencies to which student loan data may be transferred or who may gather it on behalf of the University.

Departmental Security Administrator

The Departmental Security Administrators (DSA) for each Boston University department that handles customer information will coordinate compliance efforts. Please refer to the Boston University Information Security Policy and the Data Protection Standards for a more detailed definition of the establishment of Departmental Security Administrators (DSA), Data Trustees and information security management.

Compliance Procedures

In each affected area, the DSA will identify and assess all levels of risk to University customers and implement the following procedures to insure compliance. It is the responsibility of the Data Trustee to evaluate and assess the risks of any changes made with regard to services offered, implementation of new procedures, policies or services and to make the necessary changes and/or adjustments to insure continued compliance.

Within each area, the DSA will regularly assist the Data Trustee to monitor and test this Program to insure compliance and make all necessary changes as required by the results of such testing and monitoring.

Employees will remove customer information from desktops and any areas of public access such as counters, the top of file cabinets, tables, printers, copiers and FAX machines. Offices containing customer information will be locked at night and access to offices engaged in the provision of financial services such as Student Loans, Collections, Student Accounting Services and Financial Assistance will be restricted to authorized personnel only. All promissory notes will be stored in locked, fireproof file cabinets in restricted-access, locked storage rooms where Student Loan files are stored.

With respect to electronic data, the existing Boston University Information Security Policy remains applicable to customer information protected by this Safeguarding Program, including provisions regarding password confidentiality, the periodic changing of passwords, restriction of access to personal computers and elimination of storage of customer information on generally accessible machines. Care will be taken to insure the protection of all information disseminated by FAX, data transferred electronically and data stored online.

The Family Educational Rights and Privacy Act (FERPA), the Fair Debt Collection Practices Act (FDCPA) and other laws governing the dissemination of information to third parties will be appropriately enforced. Designated personnel will monitor compliance, evaluate the effectiveness of this Safeguarding Program and collaborate with DSA's and other University officials in implementing any needed adjustments to this Program. Outside service providers will be required by contract to implement and monitor safeguards sufficient to protect customer information as required by the Gramm-Leach-Bliley Act. The sale, lease, license or other distribution of customer information, including lists, abstracts and summaries of any kind is strictly prohibited.

Disposal

Boston University requires the shredding of all paper containing any customer information prior to disposal. In the event of any recycling of personal computers containing customer information, all memory components of such computers will be completely reformatted or otherwise erased for any new use as determined by the department.

System Failures

In order to prevent breaches of this Program, assigned personnel will test data security systems governed by this Program for weaknesses, monitor performance of service providers and conduct physical security analyses of both electronic and hardcopy records. This will insure that all Program goals are being met and that University customers can be secure in the knowledge that their personal financial information is protected.

Any breaches of this program must be reported immediately to the Director of Student Loans and Collections at 617-353-4100 or the Controller at 617-353-3529, in order to assess the potential damage such breach may impose on our affected customer. Steps will be taken to re-secure information and any affected systems will be examined to insure future compliance.

Questions

Questions regarding the Gramm-Leach-Bliley Act and the Fair Debt Collection Act should be referred to the Director of Student Loans and Collections at 617-353-4100 or the Controller at 617-353-3529.

Questions and issues relating to Family Educational Rights and Privacy Act should be referred to the Office of the University Registrar at 617-353-3678.

Questions regarding the Boston University Information Security Policy should be referred to the University Information Systems (UIS) Data Security at 617-353-9004.

END OF POLICY TEXT

Additional Resources Regarding This Policy

Related Policies

- Data Protection Standards
- Sensitive Data Incident Response
- FERPA Policy
- HIPAA Policy
- Access to Electronic Information Policy
- Digital Privacy Statement
- Acceptable Use of Computing Services Policy – Effective May 23, 2023, replaced the Conditions of Use and Policy on Computing Ethics
- Network Security Monitoring Policy
- Information Security Policy
- Record Retention Policy

Additional BU Resources

- Additional Guidance on Data Protection Standards
  - 1.2.D.1 – Destruction of Paper Records and Non-Erasable Media -CD-ROMs, DVDs (Data Protection Standards Guidance)
  - 1.2.D.2 – Destruction of Individual Files on Reusable Media (Data Protection Standards Guidance)
  - 1.2.D.3 – Securely Erasing Entire Reusable Storage Devices (Data Protection Standards Guidance)
  - 1.2.D.4 – Physically Destroying Reusable Storage Devices (Data Protection Standards Guidance)

- Listing of related BU TechWeb Policies

Categories: Information Management, Privacy and Security Keywords: act, bliley, control, defend, g.l.b.a., GLBA, gramm, guard, info sec, information security, law, leach, safe

Please use this URL for the most recent version of this document: https://www.bu.edu/policies/safeguarding-information-gramm-leach-bliley-act/