

## **GLBA Security Standards for Networked Devices**

### **I. Purpose**

The purpose of the Gramm Leach Billey (GLBA) Security Standard is to provide the data protection security necessary to comply with Rutgers' GLBA Security Policy. These standards are mandatory requirements, and establish an effective baseline of appropriate system, administrative, and physical controls to apply to covered data. Specific information security guidelines and checklists are available to provide guidance on how to comply with these standards.

### **II Standard**

#### **1. Network**

- 1.1 A network based Firewall shall be implemented that denies traffic from "untrusted" networks and hosts.
- 1.2 Network traffic shall be limited to only those services and ports considered essential, unless exceptions to allow access to required services are requested and granted.
- 1.3 Networks that house devices with GLBA data shall be scanned for vulnerabilities at least semi-annually. Vulnerabilities detected shall be remediated in a timely manner.
- 1.4 Additional Security detection tools (Intrusion Detection (IDS) should be considered in cases where a high degree of GLBA data exists.

#### **2. Host**

- 2.1 Devices that process or store GLBA information shall be housed in a physically secure location, accessible to only those with a business purpose.
- 2.2 Security updates and patches shall be applied in a timely manner, or automatically when possible.
- 2.3 Computer system support must monitor for announced vulnerabilities in their hardware and software.
- 2.4 Where possible, computer anti-virus shall be implemented, and updated in a timely manner, or automatically where appropriate.
- 2.5 Where appropriate, a host based firewall shall be implemented.

## Draft

- 2.6 Services and applications should be the minimum necessary to accomplish the required business functions.
- Passwords shall be changed from the vendor defaults.
  - Systems should be “hardened” to a recognized standard, where available.
- 2.7 Individual access to data shall be limited to only those needing access for business purposes.
- 2.8 The amount of GLBA information collected and stored shall be the minimum amount required for the efficient and effective conduct of business functions.
- 2.9 Where possible, secure (encrypted) transmission and storage shall be utilized, for all devices, including laptops and portable media, where appropriate.
- 2.10 Devices processing or storing GLBA data shall log all significant security event information. Logs should be reviewed on a daily basis, and be retained for at least 90 days.
- 2.11 Files shall be backed up and tested on a regular schedule, and stored in a secured location both on and off-site.
- 2.12 Hardware, Software and data destruction shall be securely disposed at the termination of business need.

### **3. User Accounts**

- 3.1 A process shall be established to create and assign, maintain, and verify a unique system identifier (i.e. UserID) for each user.
- 3.2 Authentication to a system identifier shall be controlled by a mechanism implemented based upon the sensitivity of the data.
- 3.3 In cases where UserID and Password are used for authentication purposes, whether for interactive or file transfer purposes, the password must be encrypted.

### **4. Software Development**

- 4.1 Internally developed software shall be based on secure coding guidelines, and reviewed for common coding vulnerabilities.

## **5. Policy and Procedure**

- 5.1 Each department processing or storing GLBA data shall establish a security policy, and corresponding procedures to address the following.
- Computer Incident Response
  - Computer Incident Reporting
- 5.2 Each department processing or storing GLBA information shall provide security awareness training (i.e. seminar, podcast, etc) on an annual basis.
- 5.3 Each external vendor processing or storing GLBA data will be required to meet the security requirements set forth in this standard.

## **Glossary**

**Authentication:** The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

**Availability:** To ensure that the information remains accessible to authorized users.

**Baseline Requirement:** A baseline requirement is a requirement that represents a minimum security requirement from a body of minimum requirements. Baseline requirements are directed at maintaining a minimum level of security.

**Baseline Control:** A baseline control is a minimum security control.

**Confidentiality:** To ensuring that only authorized people have access to information.

**Data Owner:** Department head, manager or delegate within the University who has responsibility and authority for a particular set of information

**“Hardened”:** The process of securing a system, which is done to protect systems against attackers.

**Server(s) :** Computer systems engaged in providing data or services across the network.

**User(s):** – Users are identified as all individuals who make use of Rutgers University