

University of Georgia
Customer and Personal Information Security Program
Self Assessment

GLBA refers to a law called the Gramm-Leach-Bliley Act established by the Federal government. One of the government's goals under GLBA is to assist financial institutions in protecting the security of individuals' non-public financial information. Although the University of Georgia is an educational institution, it is required to comply with GLBA regulations that dictate how it safeguards non-public financial information. As a part of its compliance efforts, the university is undertaking a broader review to determine all of the departments/units that handle "personal information."

Your assistance is needed to help identify reasonable foreseeable external and internal risks to the security, confidentiality, and integrity of data that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of information. The attached questions have been provided to assist in your evaluation of risk.

In answering these questions, it is very important that you understand the meaning of some terms used in relation to GLBA.

- **Individual:** For this policy an individual includes anyone who receives a financial service from the university and who, in the course of receiving that financial service, provides the university with non-public financial information about themselves. Individuals may include, but are not limited to, students, parents, faculty, staff and other third parties with whom the university interacts.

- **Personal information:** Personal information means any non-public financial information about an individual that is handled or that is maintained by or on behalf of the university or its affiliates. The definition of personal information is very broad and may include:
 - social security numbers
 - credit card numbers
 - bank account numbers
 - account balances
 - credit history or rating
 - tax return information
 - student grades (FERPA)
 - medical records (HIPPA)

Date _____

Information Security Survey

Department/Unit Name _____

Campus/Location _____

Point of Contact for Business Processes _____

Phone Number _____

Point of Contact for Info Tech Processes _____

Phone Number _____

Physical Security

1. Does your office use, receive, maintain, transmit or store personal information?

Yes No

2. Check off the types of information your office uses, receives, transmits, stores or maintains.

- social security numbers
- credit card numbers
- bank account numbers (note account numbers are recorded on the bottom of checks your office may receive.)
- account balances
- credit history or rating
- tax return information
- staff/faculty evaluations
- student grades and/or academic evaluations of students (FERPA)
- medical records (HIPPA)
- Other _____

3. If your office receives personal information, from whom does it receive this information and how is it received? (ex. from parents by mail, from banks electronically, etc.)

4. If your office transmits personal information, how is this information transmitted?

Phone Fax Web page E-mail
Mail Hand-delivery Credit card terminal
Direct-dial connection to another computer
Other _____

5. Does your office use personal information in any way not listed above? If so, how is it used?

6. What security procedures/requirements does your office use or have in place to safeguard the personal information your office uses, receives, transmits, stores or maintains? (ex. - kept in filing cabinet in office with restricted access, kept in office locked at night, locked in cage, computer screens turned to avoid inadvertent viewing, password protected, electronic data is encrypted, responding to requests over the phoneetc.)

7. Based on the sensitivity of the information used, do you believe the data is necessary and that there are no alternatives?

8. How long do you retain the personal information before disposing of it? (ex. - kept until processed, kept until student graduates, kept X number of years, kept indefinitely)

9. How does your office dispose of personal information? (ex. - shredded, put in trash or recycle bin, incinerated, deleted from computer, sent to archives, etc.)

Electronic Security

10. Do you store, process or transmit the following personal information on your unit's network or computers?
- a. social security numbers
 - b. credit card numbers
 - c. bank account numbers (note account numbers are recorded on the bottom of checks your office may receive.)
 - d. account balances
 - e. credit history or rating
 - f. tax return information
 - g. staff/faculty evaluations
 - h. student grades and/or academic evaluations of students (FERPA)
 - i. medical records (HIPPA)
 - j. Other _____
11. Has the security of your department's local area network / computers been evaluated?
- When?
12. What procedures, practices and/or software do you use to prevent system compromises?
13. What procedures, practices and/or software does your unit have that would alert your office that your network or computer has been compromised?
14. Has your network or computer ever been compromised?
15. What are your procedures if you suspect your network or computer has been compromised?
16. How do staff members get assigned UserIDs and passwords?
Is it necessary to change passwords periodically?
Is staff provided guidance on how to develop a password?

17. What data processed on departmental computers is confidential/sensitive yet mission critical?

18. How are computers protected from viruses?

19. What are the procedures for insuring that the systems have the most current patches?
Are your systems currently up-to-date?

20. Describe the backup process for data. How often are backups performed? Where are backups kept?

21. Do you have computer labs for students? How is the lab equipment protected?
(Physically and Electronically)

If you have any concerns, questions or are not sure whether your department/unit is using receiving, transmitting, storing or maintaining personal information properly contact:

The Internal Auditing Division
706-542-1494

Send completed surveys to:

Internal Auditing Division
240 S Hull Street
Athens, GA 30677

Or
dwetzel@uga.edu

Put “**Info Survey**” in the subject line