



The University of Georgia

Privacy Policy

Organizational Function	UGA Information Assurance	Policy Number	MM-YYYY- Prog/Sys/Issue
Policy Category	Program Policy	Issue Date	09-17-2009
		Effective Date	01-07-2009
Subject	UGA Privacy Policy		
		Review On	In Review
Office of Primary Responsibility	UGA Office of Information Security	Authorized By	ITMF SecComm
Address	University of Georgia Computer Services Annex Athens, Georgia 30602-1911	Responsible Official	Brian Rivers
Distribution	University-wide	Phone	706-524-3106
		Fax	706-524-0349
On-Line Publication	https://infosec.uga.edu/policies/	Web	infosec.uga.edu
		Status	Ratified

1 Overview

The University of Georgia is committed to the responsible use of sensitive information collected from and about its students, faculty, staff, business partners and others who provide such information to the university. This commitment is in accordance with both state and federal regulations concerning the use of sensitive information. Such sensitive information includes information that could be used to cause financial harm or reputational harm to any individual. This policy applies to personally identifiable sensitive information and how it is collected.

2 Objective / Purpose

The purpose of this policy is to protect the privacy of individuals who have sensitive information stored (either in electronic or paper form) on assets owned by The University of Georgia, while at the same time providing the University the ability to share this information with authorized entities as required by policy or law.

3 Scope

The UGA Privacy Policy applies to all faculty, staff, students, affiliates, prospective students, contractors and sub-contractors who interact with UGA systems and processes, electronic or otherwise.

4 Policy

4.1 Limits on Use and Access

The responsible use of sensitive information requires that the University respect individual privacy, protect against identity theft and other unauthorized uses, and comply fully with all laws and government regulations in the collection, use, storage, display, distribution and disposal of such information. Authorized uses of sensitive information within the University are limited to uses which a) are necessary to meet legal and regulatory requirements; b) facilitate access to services, transactions, facilities and information; or c) support efficient academic and administrative processes.

Access to sensitive information is limited to:

- the individual whose information is produced or displayed;
- a University official or agent of the University with authorized access based upon a legitimate academic or business interest and a need to know;

- an organization or person authorized by the individual to receive the information;
- a legally authorized government entity or representative;
- other circumstances in which the University is legally compelled to provide access to information, such as the Georgia Open Records Act;
- or other individuals or entities, as allowed by law, for purposes judged to be appropriate or necessary for the reasonable conduct of University business

4.2 Social Security Numbers

Social Security numbers are always considered confidential and are therefore subject to the access restrictions described above. The University will continue to collect and maintain Social Security numbers in all instances in which that number is required by law for reporting or other uses. This includes, but is not limited to, all enrolled students who are U.S. citizens or permanent residents. In addition, the University will continue to use Social Security numbers, as allowed by law, for operational purposes for which there is no reasonable substitute.

The University, its faculty, staff, and students must abide by all state legal regulations pertaining to Social Security Number protection.

It is against both state law and University policy to:

- Publicly post or display the Social Security number in any manner;
- Require an individual to transmit his or her Social Security number over the Internet unless the connection is secure or the number is encrypted; or
- Require an individual to use his or her Social Security number to access an Internet site unless a unique password or PIN is also required.

This Privacy Policy also prohibits the following:

- Printing the Social Security number on any card required to access services; or
- Establishing a new process that requires the printing of a Social Security number on any materials that are mailed unless required by other state or federal agency.

4.3 Online Collection of Sensitive Information

University departments that collect sensitive information on their Web pages must post a link to the UGA Privacy Policy and inform consumers about any persons or entities outside the University with whom they may share Sensitive Information collected online. If there is a process for the consumer to change such information, that process must be described and available to the consumer on the department Web pages. Any changes to this privacy policy will be posted on the Web site.

4.4 Personal Biomedical and Human Subjects Information

Medical records, records pertaining to personal health information and records pertaining to human subjects in research projects are governed by more extensive restrictions.

For more information regarding medical records and records containing personal health information, refer to <http://www.usg.edu/legal/hipaa/practices.phtml>

For more information concerning human subjects' research, refer to <http://www.ovpr.uga.edu/compliance/hso/guidelines/4>

4.5 Federal Education Rights and Privacy Act

The Federal Education Rights and Privacy Act (FERPA) is a federal law designed to protect the privacy of education records and provides students with certain rights with respect to their education records. For more information concerning the privacy of student records refer to the University of Georgia's FERPA Compliance policy at <http://www.reg.uga.edu/or.nsf/html/ferpa>

4.6 Other Existing Information Management Policies on Campus

This policy is not intended to replace existing University of Georgia policies relating to the use and maintenance of sensitive information. In addition to the policies listed in Section 4.4 and 4.5 above, please refer to the following websites for further information regarding existing policies:

Gramm-Leach-Bliley Act (GLBA)

<http://www.uga.edu/audit/glba/policy.html>

Criminal Background Check Policy

<http://askuga.uga.edu/default.asp?id=1637&Lang=1&SID=>

5 Enforcement

Enforcement of this policy is the responsibility of the Office of the Chief Information Officer and the Office of the Chief Information Security Officer.

5.1 Policy Roles & Responsibilities

Department and/or Unit Responsibility

Each University department/unit is responsible for reviewing and monitoring internal procedures, reports and other documents to assure compliance with the UGA Privacy Policy.

This responsibility includes providing training and control systems for the responsible use of sensitive information that is accessible to its employees. The University encourages all individuals to exercise caution in making available their own sensitive information to others. In particular, individuals should not give others access to their identification cards, passwords or personal identification number (PIN).

5.2 Consequences & Sanctions for Non-Compliance

Any student, faculty, or staff member found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment or expulsion from the University. Violation of this policy may result in termination of contracts or commitments to vendors and other affiliates. Legal action may be pursued where appropriate.

6 Review and Measurement

The CISO, in cooperation with the ITMF-SECCOMM, will review the policy and standards on an annual basis.

This policy may also be used for auditing purposes by the UGA Office of Internal Audit (IT Audit) team.

7 References

What is Sensitive Information?

<https://infosec.uga.edu/sate/sensitive.php>

UGA Password Policy

https://infosec.uga.edu/policies/documents/UGA_Password_Policy_v3.8.4.pdf

Protection from disclosure social security number(s) O.C.G.A 10-1-393.8

<http://law.justia.com/georgia/codes/10/10-1-393.8.html>

Veterinary Records – O.C.G.A. 24-9-29

<http://law.justia.com/georgia/codes/24/24-9-29.html>

Georgia Open Records Act

http://www.uga.edu/news/open_records

Laws Relevant to Information Security

<https://infosec.uga.edu/policies/laws.php>