Protecting Personal Identifying Information

Introduction and Policy Purpose

The S.C. Financial Identity Fraud and Identity Theft Protection Act went into effect on December 31st, 2008. Under this law we are required to protect all "personal identifying information", which includes a **name** combined with a **SSN**, **driver's license** or **ID card number**.

Policy Statement

The division of Information Technology & Services has established a policy regarding acceptable use of personal identifying information. This policy is intended to protect individuals' privacy while using technology to collect, store, process and utilize personal information in the pursuit of university goals. It is our intention to continually evaluate how services affect privacy and take action to reduce any identified privacy risk.

This policy is in reference to the following:

- Restrictions on the use of social security numbers
- Requirements to protect personal identifying information during transfer or disposal
- Requirements to notify when a security breach occurs

Restrictions on the use of social

One objective of the OneCarolina system is to eliminate the use of SSN as a key system identifier. The OneCarolina Sponsors have asked that all systems using SSN as a key identifier today migrate to USC ID or GUID for the 2013-2014 academic year, Until that happens, please be conscious of how you use any personal identifying information and follow these guidelines:

- Do not send any personal identifying information in an email, even on campus, unless it is encrypted or password protected.
- Do not ask anyone to transmit personal information over the Internet unless it is encrypted, password protected or the connection is secure.
- Do not copy/scan documents with personal information and email them unless you block out a portion (restrictions apply to use of full social security number or six or more digits of the number) of the personal identifying information before copying/scanning. *(The ITS team is evaluating a secure scanning solution for use with our multifunction printers on campus and will share that information as soon as it is implemented and tested.)*
- Do not store personal identifying information on your local computer.
- If you are storing personal identifying information on any network drive, make sure the document is password protected and that the password is secure. In the future when Information Systems provides data to departments via a shared network drive, documents containing SSNs (plus other documents at the discretion of Information Systems) will be placed in a password-protected zipped folder that will require the user to enter a password in order to extract the document. The extracted document should not be moved or copied outside of this protected folder and should be deleted when it is no longer needed. The password for the zipped folder will be provided to the user in a separate communication.

- Do not store personal identifying information in documents on flash drives unless the drive is encrypted and the file is password protected.

Procedures to protect personal identifying information

- To password protect an Office document please see the following instructions: http://www.uscupstate.edu/campus_services/it/its.aspx?id=39218
- To password protect an Adobe PDF document please see the following instructions: http://www.uscupstate.edu/campus_services/it/its.aspx?id=39239
- Shred paper and delete files containing personal identifying information after use.

Security Breach

A "breach of the security of the system" means unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromises the security, confidentiality, or integrity of personal identifying information maintained by the person, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to a resident." S.C. Code § 1-11 11-490(D)(2)

- **Immediately report any suspected breach to the Office of the Vice Chancellor for Information Technology & Services.**

Related Policies

See also:

University Policy IT 1.06
University Policy IT 3.00