Safeguards for Dealing with Sensitive Information

This document covers how to handle, protect and safeguard the University's sensitive information.

SAFEGUARDING SENSITIVE INFORMATION

News stories surrounding identity theft and violations of privacy laws (e.g. FERPA) following the careless release of sensitive data or information are common place. To avoid potential identity theft, University liability and the litigation that sometimes follow these incidents, sensitive information, both electronic and paper, must be protected. The unintentional disclosure of personal information can cause considerable damage to the victim. The most important safeguard is to use common sense when dealing with any documents in your custody, treating them as though they contain your own private information.

Do I really need to collect information that is or may be sensitive? If the information is necessary for accomplishing a specific job or task, the answer is "yes". However, if collecting that information only when needed will have a minimal impact on job efficiency or if other less sensitive information could just as easily be used, the answer is "no." For example, a Student or Faculty ID might substitute for a Social Security Number with little or no impact; and its use outside the University environment is nearly meaningless.

We suggest that electronic documents and spreadsheets containing sensitive personal information be password protected. If needed, write down your document password(s) and lock them in a filing cabinet or desk drawer for safe keeping. Passwords for documents used only once or twice a year can easily be forgotten. **It is important to note that there are no password resets for secured documents.**

Documents stored on your network O: drive are available to others working in your department or area. Documents stored on your network P: drive are available for your use only, however, documents containing sensitive information should still be password protected for added security. Documents stored on your local hard or C: drive are only as secure as the unit itself. In any case a secured document that falls into the wrong hands will be useless without a password.

Paper forms or documents containing sensitive information should be secured in a locked file cabinet or other appropriate device. Documents that are no longer needed should be shredded to insure that they are no longer accessible. If you have questions about the retention of potentially sensitive information, contact the SU Human Resources Office with employee information questions and the University Registrar about student information.