3356-4-13 Sensitive information/information security.

Previous Policy Number:	4012.01
Responsible Division/Office:	Information Technology Services
Responsible Officer:	Associate VP and Chief Technology Officer
Revision History:	March 2009; June 2013; June 2015
Board Committee:	University Affairs
EFFECTIVE DATE:	**June 17, 2015**
Next Review:	2020

(A) Policy statement. Youngstown state university ("YSU" or "university") creates and maintains sensitive information as part of normal operations. Appropriate safeguards and procedures protect the integrity, availability, and confidentiality of sensitive information. All university employees and individuals who have access to sensitive information have a responsibility to properly handle and secure such information.

(B) Purpose. To establish guidelines for the identification and safeguarding of sensitive information (i.e., information that should not be disclosed within or beyond Youngstown state university without proper authorization and safeguards).

(C) Scope. This policy applies to university employees, customers, volunteers, vendors, contractors, board members, university affiliates, and any others who use or are allowed access to university sensitive information.

(D) Definitions and information classifications (for the purposes of this policy).

(1) "Sensitive information." Information that the university has a legal, regulatory and/or business interest obligation to protect. Sensitive information transcends the medium on which it is stored or communicated and is sensitive regardless of whether it is in verbal, paper, electronic, or any other format.

(2) "Personal information." Highly sensitive information that the university is required to protect often due to governing laws, including Family Educational Rights and Privacy Act ("FERPA"), Gramm-Leach-Bliley Act ("GLBA"), Health Insurance Portability and Accountability Act ("HIPAA"), and payment card industry

data security standard ("PCI DSS"). Compromise of personal information has specific negative consequences and requires that the university take specific actions. This category encompasses information not freely available that can be associated with a particular individual, including:

(a) Social security number.

(b) Credit card numbers.

(c) Driver's license number.

(d) Date and place of birth.

(3) "Confidential information." Sensitive information having different degrees of sensitivity but still requiring that confidentiality must be maintained. Included is information that must be very closely safeguarded, such as:

(a) Trade secrets.

(b) Employee benefit information.

(c) Student information (non-directory).

(d) Account passwords/personal identification numbers ("PINS").

(e) Digitized signatures.

(f) Encryption keys.

(g) Medical records.

(4) "YSU public information." Information that has been specifically declared and approved as public by YSU. It includes information such as student directory information to the extent permitted under FERPA or records approved as public by the general counsel's office in response to a public records request.

(E) Requirements.

(1) Sensitive information must be physically secure when not attended.

(2) Sensitive information stored or transmitted electronically must be encrypted.

(3) Sensitive information cannot be shared with unknown individuals claiming YSU association, who self-identify or reference known YSU individuals to establish their identity unless those references are checked.

(4) Communication of sensitive information by an employee requires proper procedural safeguards and the written preapproval of the department supervisor/chair and division officer/dean.

(5) Physical removal of sensitive information from YSU or its facilities requires proper procedural safeguards and the written preapproval of the department supervisor/chair and division officer/dean.

(6) Storage of YSU-related sensitive information on personally owned electronic devices by an employee requires proper procedural safeguards and the written preapproval of the department supervisor/chair and division officer/dean.

(7) All YSU employees are required to attend sensitive information and information security training.

(8) Information technology services is responsible for establishing and maintaining university information security standards, manuals, and trainings.

(F) Procedures.

(1) Take stock. Assess information in all formats to identify sensitive information. This is a responsibility of all employees having YSU-related information access.

(2) Scale down. Keep only the information that is needed to perform your job responsibilities and as identified by the YSU records retention procedure. The need to store and/or communicate sensitive information requires written approval using the "Highly Sensitive Information Storage Request" form.

(3) Lock it. Protect sensitive information in your care through actions including the following:

(a) Physically secure the information (e.g., lock physical spaces such as offices, cabinets, desks). Secure computers and other data storage devices with locks.

(b) Encrypt the information when it is stored electronically.

(c) Use only secured methods for transmitting sensitive information. (Note: email, internet, web and wireless transmissions are not secure for sensitive information by default, but steps can and must be taken to secure these methods of delivery.)

(d) Verify requester's identity and validity of requests for sensitive information communications.

(4) Pitch it. Properly dispose of information not needed to perform job duties. Proper disposal techniques include shredding or electronically wiping files. Note that deleting files electronically and/or reformatting drives are not proper disposal techniques.

(5) Plan ahead. Take positive measures to ensure proper response to potential sensitive information incidents. For example, know and document who has been granted access to what sensitive information. Have appropriate software installed on computers, cell phones, and other devices. Identify appropriate notification paths to pursue if sensitive information is compromised (including the office of the general counsel if personal information is compromised). Use change in responsibilities and resources as an opportunity to begin again at paragraph (G)(1) of this rule as part of continuous quality improvement planning.