YOUNGSTOWN STATE UNIVERSITY

RESOLUTION TO MODIFY SENSITIVE INFORMATION/INFORMATION SECURITY POLICY, 3356-4-13

WHEREAS, University Policies are being reviewed and reconceptualized on an ongoing basis; and

WHEREAS, this process can result in the modification of existing policies, the creation of new policies, or the deletion of policies no longer needed; and

WHEREAS, action is required by the Board of Trustees prior to replacing and/or implementing modified or newly created policies, or to rescind existing policies.

NOW, THEREFORE, BE IT RESOLVED, that the Board of Trustees of Youngstown State University does hereby approve the modification of the University Policy stated above and attached hereto.

Board of Trustees Meeting

June 18, 2026

YR 2026-120

3356-4-13 Sensitive information/information security.

Responsible Division/Office:	Information Technology Services
Responsible Officer:	Associate VP and Chief Information Officer
Revision History:	March 2009; June 2013; June 2015; June 2021; June 2026
Board Committee:	University Affairs
Effective Date:	**June 18, 2026**
Next Review:	2031

(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 the university without proper authorization and safeguards).

(C) Scope. This policy applies to university employees (including student employees, customers, volunteers, vendors, contractors, board members, university affiliates, and any others who use or are granted 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. Examples include personal information as defined in paragraph (D)(2) of this rule; confidential information as defined in paragraph (D)(3) of this

rule; and any other information whose unauthorized disclosure or use would create legal, regulatory, contractual, financial, or reputational exposure for the university.

(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), the Gramm-Leach-Bliley Act (GLBA), the 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: social security numbers, credit card numbers, driver's license numbers, dates and place of birth, bank account and routing numbers, passport and visa numbers, state-issued identification numbers, biometric identifiers, health insurance identification numbers, and tax identification numbers (including individual taxpayer identification numbers and employer identification numbers).

(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: trade secrets, employee benefit information, student information (non-directory), account passwords and personal identification numbers (PINs), digitized signatures, encryption keys, medical records, records of pending or threatened litigation, audits, investigations, donor and prospect information, vendor contract pricing and proprietary terms, cybersecurity vulnerability information and incident details, and information protected by attorney-client privilege.

(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 secured 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 shall complete monthly information technology security training, which shall include instruction on the handling of sensitive information.

(8) The chief information security officer or a designated qualified individual appointed in writing by the chief information security officer shall have direct accountability for overseeing, implementing, and enforcing the university's information security

program in compliance with applicable law, including the GLBA Safeguards Rule (16 C.F.R. 314). The chief information security officer shall report to senior leadership at least annually on the status of the program.

(9) Multi-factor authentication (MFA) is required for:

(a) All access to systems containing customer financial information subject to the GLBA;

(b) All administrative access to systems within the payment card data environment;

(c) All remote access to university systems containing sensitive information. MFA requirements shall be implemented and enforced by information technology services and documented in the university's information technology security manual. Exceptions require written approval from the chief information security officer and must include documented compensation controls.

(10) Access to sensitive information shall be granted on a need-to-know basis, limited to the minimum necessary to perform assigned job duties. Access controls shall include:

(a) Unique user identification for all individuals accessing sensitive systems (shared or group accounts are prohibited);

(b) Prompt revocation of access upon termination, transfer, or change in responsibilities;

(c) Periodic access reviews conducted at least annually by system owners and department supervisors; and

(d) A formal access request and approval process documented by information technology services.

(11) Sensitive, personal, and confidential information cannot be stored or transmitted using information systems, cloud services, or software applications that have not been sanctioned by information technology services.

(F) Procedures.

(1) Information inventory. Assess information in all formats to identify sensitive information. This is the responsibility of all employees with access to YSU information.

(2) Data retention. Sensitive information shall be retained only for as long as necessary to fulfill the purpose for which it was collected, or as required by applicable law, whichever is longer. Retention periods for each category of sensitive information are defined in the YSU records retention schedule. Upon expiration of the applicable retention period:

(a) Physical records must be destroyed by cross-cut shredding or equivalent method;

(b) Electronic records must be securely deleted using methods that prevent recovery;

(c) Deletion must be documented and records retained.

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

(a) Physically secure 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. Encryption methods shall meet current industry standards as defined in the university's informational technology security manual, addressing:

(i) Strong encryption of stored sensitive information and information in transit;

(ii) Secure management of encryption keys; and

(iii) Additional protections for payment card information consistent with payment card industry data security standard requirements.

(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 the requester's identity and validity of requests for sensitive information communications.

(4) Information disposal. Properly dispose of information not required to perform job duties. Proper disposal techniques include shredding or securely erasing electronic files. Note that deleting files electronically and/or simple reformatting of electronic media are not proper disposal techniques.

(5) Incident response plan. The university shall maintain a written incident response plan (IRP), reviewed and updated at least annually, that includes:

(a) Defined roles and responsibilities for response team members;

(b) Procedures for detecting, containing, and eradicating security incidents;

(c) Internal escalation to the chief information security officer, general counsel, and senior leadership within twenty-four hours of confirmed incident;

(d) Breach notification procedures per paragraph (G) of this rule;

(e) Evidence preservation procedures; and

(f) Post-incident review and lessons-learned documentation. The IRP shall be tested at least annually through tabletop exercises.

(6) All third-party vendors, contractors, and service providers that access, store, process, or transmit university sensitive information must:

(a) Execute a written agreement with YSU prior to access that includes data protection requirements no less stringent than this policy;

(b) Demonstrate adequate security controls upon request through certifications, audits, or equivalent evidence;

(c) Report any actual or suspected breach of university data to the chief information security officer within twenty-four hours of discovery. Information technology services shall maintain a vendor inventory and conduct periodic risk assessments of vendors with access to sensitive information.

(G) Breach notification.

(1) Upon confirmation of a breach of sensitive or personal information, the university shall:

(a) Notify affected Ohio residents in the most expedient time possible, and no later than forty-five days following discovery, unless law enforcement requests a delay;

(b) Notify the Ohio Attorney General prior to or simultaneously with notifying affected individuals if the breach affects one thousand or more Ohio residents;

(c) For breaches involving individuals residing outside Ohio, the university shall comply with all applicable state, federal, and international notification laws, including required notifications to attorneys general and other regulatory bodies.

(d) Where the breach involves European Union residents' personal data, notify the applicable supervisory authority within seventy-two hours of becoming aware of the breach, and notify affected individuals without undue delay where risk levels are high;

(e) Notification shall include: nature of breach, categories and approximately number of individuals affected, contact information, likely consequences, and measures taken to address the breach.

(2) The chief information security officer shall lead the university's breach response in coordination with the office of general counsel. All suspected breaches shall be reported immediately to the chief information security officer.

(H) Enforcement.

(1) The chief information officer may suspend or restrict an individual's or a device's access to university information systems and network resources when:

(a) The action is necessary to maintain the security or functionality of university information resources;

(b) The action is necessary to protect the university form potential liability; or

(c) The account, system, or device is believe to have been compromised or is in violation of this policy.

(2) The chief information officer shall promptly report any enforcement action taken under paragraph (H)(1) if this rule, together with the justification for that action to the vice president of student affairs, the vice president for finance and business operations, the provost (or their designee), or the vice president for human resources, as applicable. Technology access may be permanently suspended until due process has been completed by student conduct, the employee discipline process, or law enforcement agencies.

(3) Violations. An employee may be held financially liable for a data breach resulting from the use of non-university storage or email. In the event of a data breach, the university may decline to defend or support any employee who used unsupported information technology or engaged in unacceptable use of generative artificial intelligence. Violations of this policy are subject to disciplinary action, up to and including immediate termination. Employees who violate the university's email usage policy may also lose access to their university email account and other associated privileges.