



RESOLUTION TO MODIFY IDENTITY THEFT RED FLAG POLICY, 3356-4-14

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

September 17, 2026

YR 2027-11

3356-4-14 Identity theft red flags.

Responsible Division/Office: Finance and Business Operations
Responsible Officer: VP for Finance and Business Operations
Revision History: December 2010; December 2015; March 2021;
September 2026
Board Committee: Finance and Facilities
Effective Date: September 17, 2026
Next Review: 2031

- (A) Policy statement. The university will establish an identity theft prevention program pursuant to the Fair and Accurate Credit Transactions Act (FACTA) and its implementing federal regulations, commonly known as the federal red flags rule. The program is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or existing covered account within the university. The program is commensurate to the size and complexity of the university as a creditor.
- (B) Purpose. The purpose of this policy is to enable appropriate university officials to develop and implement policies and procedures to address the risks of identity theft to its students, faculty, staff, vendors and other customers.
- (C) Definitions. All terms used in this policy that are defined in FACTA shall have the same meaning provided therein.
- (D) Parameters.
 - (1) The requirements of this policy apply to all university departments and organizations, which regularly arrange for the extension, renewal or continuation of credit; defer payment for services rendered and/or regularly extend, renew or continue credit; furnish information to consumer reporting agencies; or use consumer reports to conduct credit or background checks on prospective employees.
 - (2) This policy incorporates by reference university policies and procedures to the extent necessary to accomplish the purpose of this policy and to comply with FACTA, including but not limited

to the following rules of the Administrative Code:

- (a) Rule 3356-3-04, “Contract compliance and administration”.
 - (b) Rule 3356-3-08, “Cash collection sites”.
 - (c) Rule 3356-4-09, “Acceptable use of university technology resources”.
 - (d) Rule 3356-4-13, “Sensitive information/information security”.
 - (e) Rule 3356-9-06, “Professional conduct of faculty, department chairpersons, and professional/administrative employees”.
- (3) At a minimum, the university’s identity theft prevention program will include:
- (a) Guidelines for identifying patterns, practices or specific activities that indicate the possible existence of an identity theft.
 - (b) Identification of reasonable and appropriate action steps that will be taken when a pattern, practice or specific activity has been detected.
 - (c) Processes requiring that accounts accessed or managed by external vendors on behalf of the university have implemented an appropriate program.
 - (d) Training to educate employees whose job is pertinent to the program as described in paragraph (D)(1) of this policy.
 - (e) Periodic review and updates to the program.
 - (f) Annual program reporting to appropriate university leadership.
 - (g) Procedures for responding to a notice of address discrepancy received from a consumer reporting agency, as

required by federal law.

- (4) In administering the program, the vice president for finance and business operations (chief financial officer) shall:
 - (a) Assign specific responsibility for the program's implementation.
 - (b) Review reports prepared pursuant to paragraph (D)(8) of this policy.
 - (c) Approve all material changes to the program as necessary to address changing identity theft risks.
- (5) The program shall include procedures to ensure that the activities of service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts.
- (6) The program shall include relevant red flags from the following categories as appropriate:
 - (a) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services.
 - (b) The presentation of suspicious documents.
 - (c) The presentation of suspicious personal identifying information.
 - (d) The unusual use of, or other suspicious activity related to, a covered account.
 - (e) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.
- (7) The program shall provide for appropriate responses to detected

red flags to prevent and mitigate identity theft. The response shall be commensurate with the degree of risk posed. Appropriate responses may include:

- (a) Monitor a covered account for evidence of identity theft.
 - (b) Contact the customer.
 - (c) Change any passwords, security codes or other security devices that permit access to a covered account.
 - (d) Reopen a covered account with a new account number.
 - (e) Not open a new covered account.
 - (f) Close an existing covered account.
 - (g) Notify law enforcement.
 - (h) Notify the university's information security office and comply with applicable breach notification requirements under rule 3356-4-13 of the Administrative Code and all other applicable federal, state, or international law.
 - (i) Determine no response is warranted under the particular circumstances.
- (8) Program reports. Each annual report shall address material matters related to the program and shall evaluate:
- (a) The effectiveness of the program in accomplishing its purpose.
 - (b) Any service provider arrangements.
 - (c) Any significant incidents involving identity theft that may have occurred and the university's response to those incidents;
 - (d) All recommendations for material changes to the program.