

## IDENTITY THEFT PREVENTION POLICY

The Board of Trustees of Salem State University recognizes that some activities of the university are subject to the provisions of the Fair and Accurate Credit Transactions Act and its “Red Flags” rules. This Identity Theft Prevention Policy, adopted by action of the board, shall guide development of guidelines and procedures to comply with Red Flags rules.

**I. Program Adoption.** Salem State University has adopted this initial Identity Theft Prevention Program (“Program”) in compliance with the Red Flags rules issued by the Federal Trade Commission pursuant to the Fair and Accurate Credit Transactions Act (“FACTA”) in recognition of the fact that the university is engaging in activities that are covered by the FACTA Red Flags rules. After consideration of the size and complexity of the university’s operations and accounting systems and the nature and scope of the university’s activities, the board determined that this program is appropriate for the university.

**II. Program Purpose.** Under the Red Flags rules, the university is required to establish an “Identity Theft Prevention Program” with reasonable policies and procedures to detect, identify, and mitigate identity theft in its covered accounts. The university must incorporate relevant Red Flags procedures into a program to enable the university to detect and respond to potential identity theft. The university shall ensure that the program is updated periodically to reflect changes in risks to customers, creditors or the university from identity theft.

**III. Responsible University Official.** The president shall designate a senior university official to serve as Program Administrator (PA). The PA shall exercise appropriate and effective oversight over the program and shall report regularly to the president on the program.

**IV. Program Administration and Maintenance.** The PA is responsible for developing, implementing and updating the program throughout the university. The PA will be responsible for: coordinating appropriate training of university staff on the program; advising on appropriate procedures to follow for identifying, preventing, and mitigating identity theft; determining which steps of prevention and mitigation should be taken under particular circumstances; serve as facilitator and advisor on incidences of identity theft and coordinate any reporting requirements, as necessary; and recommending to the president periodic changes to the program.

The program will be periodically reviewed and updated to reflect changes in identity theft risks and technological changes. The PA will consider the university’s experiences with identity theft; changes in identity theft methods; changes in identity theft detection, mitigation and prevention methods; changes in types of accounts the university maintains; changes in the university’s business arrangements with other entities, and any changes in legal requirements in the area of identity theft. After considering these and other factors, the PA will determine whether changes to the program are warranted.

The PA shall confer with all appropriate university personnel and knowledgeable experts in the area of privacy issues as necessary to ensure compliance and maintenance of an effective program. The PA shall annually report to the president on the effectiveness of the program. The PA shall present any recommended changes to the president for approval. The president’s approval shall be sufficient to make changes to the university’s Identity Theft Program.

**V. Identification of Red Flags.** In order to identify relevant Red Flags, the university considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with identity theft. The following are examples of relevant Red Flags, in each of the listed categories, which employees should be aware of and diligent in monitoring for:

- A. Notifications and Warnings from Credit Reporting Agencies
- B. Suspicious Documents
- C. Suspicious Personal Identifying Information
- D. Suspicious Account Activity or Unusual Use of Account
- E. Alerts from Others

**VI. Detecting Red Flags.** The PA will develop and implement specific Red Flags detection practices, methods and protocols appropriate to meet the requirements of this program.

**VII. Responding to Red Flags and Mitigating Identity Theft.** In the event university personnel detect any identified Red Flags, such personnel shall take prescribed steps to respond to and mitigate identity theft depending on the nature and degree of risk posed by the Red Flag as identified in the Red Flags Detection Procedures.

**VIII. Staff Training and Awareness Program.** An integral part of the program entails initial and continual training and awareness of university staff to potential incidences of identity theft. To this end, university employees responsible for implementing the program shall be trained under a university sponsored awareness and training program coordinated with departmental staff, the Office of Human Resources and the PA on the detection of Red Flags and the responsive steps to be taken when a Red Flags activity is detected.

**IX. Reporting.** Appropriate staff and/or supervisors shall provide reports to the PA on incidents of identity theft and actions taken to mitigate any risks associated with Red Flags activity. A separate “Privacy Incident Report” form shall be developed to facilitate and standardize this reporting. The reporting mechanism will be communicated to all responsible employees and will also be located on the university’s web site.

**X. Service Provider Arrangements.** In the event the university engages a service provider to perform an activity in connection with one or more covered accounts, the university will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft:

1. Require by contract that service providers have such policies and procedures in place; and
2. Require by contract that service providers review the university’s program and report any Red Flags to the PA.

**XI. Reporting Requirements to the Board of Trustees.** After initial approval of this policy by the board of trustees, the president will advise the board on a periodic basis on the continued compliance of this policy and from time to time bring appropriate recommendations to the board for their consideration for revision of this policy as necessary.