SUB-PROGRAM #1: ACCOUNTING AND PURCHASING SERVICES WITHIN OPERATIONS AND SUPPORT SERVICES

Risk Assessment

A departmental risk assessment is the first step to identify any covered accounts and the potential risk(s) to these accounts. Operations and Support Services - Accounting and Purchasing Services (APS) performed an initial assessment of its business processes and identified the online employee parking program (account) that is subject to inclusion in System Administration’s Identity Theft Prevention, Detection and Mitigation Program. To APS’s knowledge, there have been no past incidents of attempted or actual identity theft or fraud being perpetrated against the parking account.

APS will conduct a risk assessment as scheduled by the Vice Chancellor for Administration, but no less than annually, to determine whether it offers or maintains covered accounts as described in INT162. The results of the annual risk assessment will be reported to the Vice Chancellor for Administration and will be used to modify System Administration’s Identity Theft Prevention, Detection and Mitigation Program.

Definitions

APS incorporates by reference the definitions set forth in INT 165 into its sub-program.

Identification of Red Flags

The responsibility for maintaining an identity theft prevention and mitigation program for the employee parking program lies solely in APS who receives payments on this account and processes refunds in a few situations. The account consists of monthly payroll deductions for employee parking agreements. Employees log in to a secure, password protected portal to setup or update their annual parking agreement. Potential risks within APS’s control that could occur would primarily involve attempts by individuals to access the online system to make changes to a parking agreement in order to obtain parking privileges.

APS has identified specific red flags that could indicate attempted or actual identity theft or fraud with regard to this account:

- An employee can’t log into the on-line parking system with his/her SNAC (password protected);
- A report that a participating employee’s SNAC (password protected) has been stolen or otherwise compromised;
- A complaint or question from an employee based on the employee’s payroll deduction for parking that the employee denies authorizing;
- The employee’s parking permit was stolen or is missing;
- A inquiry from a participating employee that a parking sticker or card was never received; or
- A participating employee claims to be the victim of any type of Identity Theft.
Detecting Red Flags

Methods of detection of Red Flags include:
- Requiring an employee to provide photo identification at each “in person” encounter;
- Requiring that on-line transactions come though a secure, password protected portal or in the case of a System Administration employee, a verifiable, secure password protected System Administration e-mail account; or
- Following up on each payroll deduction inquiry from employees regarding payroll deductions for parking not requested by the employee.

Preventing and Mitigating Identity Theft

When a red flag is detected by an APS employee or who otherwise becomes aware of possible activity that indicates potential or existing fraud or identity theft with regard to the employee parking program shall notify the Director of APS. Upon receipt of such a report, the Director of APS will log the report and gather all available information regarding the transaction, and take any or all action determined to be reasonable under the circumstances to prevent or mitigate identity theft with regard to the employee parking program.

Updating the Program

APS’s identity theft prevention program will be updated to reflect changes in operations and changes in potential risks of identity theft no less than annually by the Director of APS.

Training

APS employees will be trained upon hire and receive annual refresher training on APS’s Identity Theft Prevention Program. The Director of APS is responsible for developing this training and ensuring employees receive this training.