ADM 410
Security Policy #10

Facility Security Plan

Purpose of Policy

The purpose of the policy is to define the procedures that will limit physical access to PII and sensitive company data and the facility or facilities in which such systems are housed, while still ensuring that proper authorized access is allowed.

Facility Security Plan

1) Physical security of office buildings must be implemented to protect PII and sensitive data as well as other company assets. Physical measures might include: surveillance camera, fences, locked gates / doors, etc.

2) All systems that store or access PII and/or sensitive company data should be stored in locked rooms, closets or cabinets to prevent unauthorized access. Access to these facilities should be minimized and limited to only employees and/or vendors that need access to perform their job function.

3) Where practical, all visitors should be restricted from areas where files or systems containing PII and/or sensitive company data are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files or systems containing PII and/or sensitive company data are stored.

4) A clean desk policy will be implemented and includes the following: All employees are prohibited from keeping unsecured paper files containing PII and sensitive company data in their work area when they are not present (e.g. lunch breaks). At the end of the day, all files containing PII and/or sensitive company data are to be stored in a locked filing cabinet, desk drawer or other locked location. Any systems that store or access PII and/or sensitive company data should be closed or access should be terminated (i.e. system logoff).

5) The Security Officer or maintenance shall maintain a secured and confidential master list of all lock combinations, passcodes, and keys. The list will identify which employee possess keys,

keycards, or other access devices and that only approved employees have been provided access credentials.