ADM 406
Security Policy #6

Access Control

Purpose of Policy

The purpose of the policy is to assure that systems containing PII and/or sensitive company data are accessed only by those persons or software programs that have been granted appropriate access rights

Unique User Identification

1) Employees will be assigned a unique user identification (i.e. user-id) in order to access any system or application that transmits, receives or stores PII and/or sensitive company data.

2) Each employee must ensure that their assigned user identification is appropriately protected and only used for legitimate access to systems or applications.

3) If an employee believes their user identification has been comprised, they must report the security incident.

4) Password complexity will be re-evaluated periodically.

5) Employees should be aware of the following procedures to protect passwords:

    a. Passwords should not be written and attached to computer for anyone to see.

    b. Passwords should not be shared with other employees

    c. If an employee suspects that their password has been compromised they should report the incident immediately

6) Password change requirements will be re-evaluated periodically.

7) After a number of failed password attempts, the employee's account should be disabled and will be re-evaluated periodically.

Automatic Logoff

1) Systems that access or store PII and/or sensitive company data should implement an automatic logoff after a determined period of inactivity. Employees would need to login again to regain access and continue the session. Automatic logoff should occur within 15-30 minutes.

2) When leaving a server, workstation, or other computer system unattended, employees must lock or activate the system's automatic logoff mechanism or logout of all applications and database systems containing or accessing PII and/or sensitive company data.

Encryption and Decryption

1) To the extent technically feasible all portable devices that contain PII and/or sensitive company data should be encrypted to protect the contents. In addition, encryption should be used when sending any PII or sensitive company data across public networks and wireless networks. Public networks include email and Internet access.

2) Employees should be trained on the use of encryption to protect PII and sensitive company data.

3) All backup tapes and media that contain PII and/or sensitive company data should utilize encryption to protect the data.

4) Secure encrypted remote access procedures should be implemented to protect systems that access or store PII and/or sensitive company data.

    a. Authentication and encryption mechanisms should be required for all remote access sessions to networks containing PII and/or sensitive company data.

    b. Two-factor authentication should be implemented where technically feasible.

5) All wireless access to networks should utilize encryption mechanisms.

    a. Employees should not utilize open public Wi-Fi networks