**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. userid) 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. Employees should be aware of the following password procedures to create and use strong passwords to protect PII and sensitive company data:
	1. Should be a minimum of eight characters in length.
	2. Should incorporate both upper and lower case letters (e.g. a-z and A-Z)
	3. Should incorporate digits and punctuation characters as well as letters e.g., 0-9, (! @ # $ % ^ & \* ( ) \_ - + = { } [ ] : ; “ ‘ | \ / ? < > , . ~ `)
	4. Should not be words found in a Dictionary.
	5. Should not include easily guessed information such as personal information, names, pets, birth dates, etc.
5. Employees should be aware of the following procedures to protect passwords:
6. Passwords should not be written down
7. Passwords should not be shared with other employees
8. If an employee suspects that their password has been compromised they should report the incident immediately
9. Passwords should be changed at least every 90 days
10. After a number of failed password attempts, the employee’s account should be disabled (e.g. 3 or 5 failed attempts)

**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 (i.e. 10 minutes of inactivity). Employees would need to login again to regain access and continue the session.
2. When leaving a server, workstation, or other computer system unattended, employees must lock or activate the system’s automatic logoff mechanism (e.g. CTRL, ALT, DELETE and Lock Computer) 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.
5. Authentication and encryption mechanisms should be required for all remote access sessions to networks containing PII and/or sensitive company data. Examples of such mechanisms include VPN clients, authenticated SSL web sessions, and encrypted Citrix/RDP client access.
6. Two-factor authentication (i.e. SMS pin notification) should be implemented where technically feasible.
7. All wireless access to networks should utilize encryption mechanisms.
8. Employees should not utilize open public Wi-Fi networks