****

#3 Information and Data Privacy

|  |  |
| --- | --- |
|  **Procedures to meet this best practice:** |  |
|  |

* Physical security of Non-public Personal Information.
	+ Restrict access to Non-public Personal Information to authorized employees who have undergone Background Checks at hiring.
	+ Prohibit or control the use of removable media.
	+ Use only secure delivery methods when transmitting Non-public Personal Information.
* Network security of Non-public Personal Information.
	+ Maintain and secure access to Company information technology
	+ Develop guidelines for the appropriate use of Company information technology.
	+ Ensure secure collection and transmission of Non-public Personal Information.
* Disposal of Non-public Personal Information.
	+ Federal law requires companies that possess Non-public Personal Information for a business purpose to dispose of such information properly in a manner that protects against unauthorized access to or use of the information.
* Establish a disaster management plan.
* ***Appropriate management and training of employees*** to help ensure compliance with Company’s information security program.
* Oversight of service providers to help ensure compliance with a Company’s information security program.
	+ Companies should take reasonable steps to select and retain service providers that are capable of appropriately safeguarding Non-public Personal Information.
* Audit and oversight procedures to help ensure compliance with Company’s information security program.
	+ Companies should review their privacy and information security procedures to detect the potential for improper disclosure of confidential information.
* Notification of security breaches to customers and law enforcement.
	+ Companies should post the privacy and information security program on their websites or provide program information directly to customers in another useable form. When a breach is detected, the Company should have a program to inform customers and law enforcement as required by law.