|  |  |
| --- | --- |
| Organizational Function Area: | Information Classification Policy |
| Board Approved: |  |
| Last Revision Date: | 6/1/2015 |
|  |  |
| Department Responsible for Policy Maintenance: | Information Technology |
|  |  |

**Scope**: This policy governs the classification of information throughout the institution and includes the transmission of data to and from third parties.

**Purpose**: To develop standard definitions for classifying the sensitivity of data in order to apply appropriate safeguards in accordance with the data’s classification.

**CLASSIFICATION LEVELS**

The following classification levels are established:

**Public**

This information is freely available to the public. Within this level no data is required to be secured from the public. This classification includes items such as our business hours, marketing messages, etc.

**Confidential**

This level of classification requires the information to be secured from public access. This includes any material with sensitive customer information. Sensitive customer information is defined as customer name, address or telephone number, in conjunction with the person’s social security number, driver’s license number, credit or debit card number, personal identification number, or password that would permit access to the customer’s account.

**Private**

This data is only available to senior management, or approved personnel. This includes information such as employee records, risk assessments, strategic plans, etc.

**REQUIREMENTS**

The term “non-public” information is used to refer to all data not considered public. This includes all data classified as **Confidential** or **Private**.

The following requirements are established to governed access to and control of non-public information. In the event that a specific issue is not addressed, employees are expected to take appropriate cautions to avoid any potential disclosure, misuse, or alteration of non-public information.

**Transmission:** All non-public information transmitted via an unsecured connection (e.g. Internet), will be encrypted to a commercially reasonable standard in order to prohibit the unauthorized access to such information.

**Disclosure:** Prior to disclosure of non-public information, the identity of the requestor, and authorization to have such information, must be confirmed prior to disclosing the information.

Call-back verification is mandatory for all third-party requests for non-public information when the identity of the caller cannot be verified. This includes requests for information from vendors, regulators, consultants, auditors, etc. The call-back will be made to a phone number of the entity that is known to be legitimate.

**Storage:** All non-public information will be stored in an institution-controlled facility or an institution-approved storage facility. Within the institution, non-public information will be secured when not in use. This includes information that is pending destruction.

**Removal:** Should non-public data need to be removed from an institution controlled or approved facility, the information will be appropriately controlled in order to prevent unauthorized access. This may include controls such as physical possession of the information by an employee, or encryption of material via a commercially reasonable means.

**Requests**: There may be times that we request others to provide non-public information to us. In these events, we will ensure that a secure method is provided or used to obtain the non-public information. Although we cannot guarantee that the other party will use a secure method, we will ensure that a secure method is available for use.

**Destruction:** When no longer needed, all non-public information will be appropriately destroyed in a manner that prohibits the recovery of the information. This includes information in any form, paper or electronic. At a minimum, paper media will be destroyed with a commercially reasonable process and electronic media will be degaussed and/or physically destroyed.

**Return/Retiring of Equipment:** If any equipment is returned or retired, any non-public data stored on the equipment will be appropriately removed via commercially reasonable method that would prevent recovery of that information. This requirement includes all leased or rented equipment.

**Cancellation of Services:** In many situations there may be third-parties that have access to, or process, non-public data on our behalf. In conjunction with the **Vendor Management Program**, all non-public data with third-parties will be returned, destroyed, or appropriately secured after the termination of services with that third-party.