|  |  |
| --- | --- |
| Organizational Function Area: | Acceptable Use Policy |
| Board Approved: |  |
| Last Revision Date: | 01/01/1999 |
|  |  |
| Department Responsible for Policy Maintenance: | Information Technology |
|  |  |

**Scope:** All employees and contractors of the institution that access non-public systems or information shall be governed by this policy.

**Purpose:** To define appropriate use of the institution’s information systems and control of information assets.

**RESPONSIBILITY**

**Business Unit Managers**

Business unit managers will ensure that each employee they supervise receives and understands this **Acceptable Use Policy**. Annually, each employee must sign a policy acknowledgement attesting to their understanding and acceptance of the policy’s requirements.

**Human Resources Department**

Ensure that all new hires are provided a copy of, and acknowledge agreement with, this policy.

**Employees and Contractors**

Comply with requirements outlined in this policy and any referenced policies.

**NON-COMPLIANCE WITH POLICY**

Non-compliance with this policy may result in disciplinary action, including termination of employment. Any activity may also be reported to authorities as appropriate.

**ACCEPTABLE USE REQUIREMENTS**

All users with access to non-public systems or information will agree to the following guidelines:

* Use institution’s systems solely for business purposes
* Maintain privacy and confidentially of all non-public information in accordance with the **Information Classification Policy**
* Not to transmit any proprietary, confidential, or otherwise sensitive information without authority
* Not to remove non-public information from institution facilities without proper approval
* Use assigned authentication credentials (user-ID/password) for access to authorized systems
* Be responsible for all activities occurring with assigned authentication credentials
* Maintain confidentiality of assigned authentication credentials
* Not to circumvent authentication mechanisms, such as login requirements
* Not to disable or attempt to circumvent security systems or software
* Log out of all systems when the system is to be unattended
* Not to connect any unauthorized devices or systems to internal networks
* Not to install any unauthorized software programs on institution systems
* Not to sign up for, or access, any unauthorized web-based services
* Not to attempt to access or use information for which you are not authorized
* Not to remotely access the institution’s systems unless authorized
* Report information security violations immediately to the Information Security Officer
* Report any loss of data or critical device to the Information Security Officer
* Notify the Information Security Officer or member of the Incident Response Team if any customers indicate they are a victim of electronic payment fraud.
* Only authorized personnel may use social media on behalf of the institution. See the **Social Media Guidelines** for guidance on personal use of social media.

Remote Users Only

In addition to the requirements detailed above, authorized remote users agree to the following requirements:

* Not to access the network from inappropriate locations where others may view information
* Not to allow others to view, use, or access information from the remote terminal
* Not to leave the remote terminal unattended at any time while connected to the internal network

**Appendix A – Acceptable Use Policy Acknowledgment**

Date:

Employee Name:

I have read, understand, and agree to the requirements and limitations detailed in the **Acceptable Use Policy.**

Signature: