**Sample Physical and Logical Access Security Policy**

**I. SCOPE**

This policy applies to all departments and offices at all locations, owned and leased, of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (“Company”). The policies and procedures provided herein apply to all Company employees, staff, visitors and contractors.

This policy governs the physical and logical access to all Company systems and applications to protect the privacy, security, and confidentiality of Company systems, especially highly sensitive systems, and the responsibilities of institutional units and individuals for such systems.

**II. DEFINITIONS**

**Access:** The ability to use, modify or manipulate an information resource or to gain entry to a physical area or location.

**Access Control:** The process of granting or denying specific requests for obtaining and using information and related information processing services or resources and to enter a specific physical facility, such as a building or designated room containing information resources.  Accompanying the process are procedures that monitor access.  The purpose of access controls is to prevent unauthorized access to IT systems.

**Availability:** Protection of IT systems and data to ensure timely and reliable access to and use of information to authorized users.

**Confidentiality:** The protection of sensitive information so that it is not disclosed to unauthorized individuals, entities or processes.

**Information Security Officer (ISO):** The individual designated by the chief information officer to be responsible for the development, implementation, oversight, and maintenance of the Company’s IT security program.

**Integrity:** The protection of data or IT so that data has not been intentionally or accidentally been modified or deleted in an unauthorized and undetected manner.

**Least Privilege:** The principle of least privilege requires that a user be given no more privilege than necessary to perform a job.  The enforcement of least privilege requires identifying what the user’s job is, determining the minimum set of privileges required to perform that job, and defining the user’s role which includes those privileges only.

**Logical Access Control:**  Logical access controls provide a technical means of controlling what information a user can utilize, the programs the user can run, and the modifications the user can make.  These controls are computer-based and can prescribe not only who or what process is to have access to a specific information resource but also the type or level of access that is permitted, such as use, change, or view.

**Physical Security:**  The physical safeguards that protect against unauthorized access, can detect attempted or actual unauthorized access and can activate an effective response.  These measures are required to control access to information resources and assets.

Depending on the classification of the information resource, the appropriate physical security safeguards such as progressively restricted security zones, locked doors, access control systems, intrusion alarm systems, and other provision will be implemented.

**Separation of Duties:** The “separation of duties” is defined as the assignment of responsibilities such that no one individual or function has control over an entire process.  The principle of “separation of duties” manages conflict of interest, the appearance of conflict of interest, and potential fraud.

**Server:** A server is a system (software and suitable computer hardware) that responds to requests across the Company’s network or the Internet, if hosted off campus, to provide, or help to provide, a network service. All systems that are intentionally configured to be accessible via the internet are considered to be servers. A system may only be accessible from the Company network but provides a server service and therefore is a server.

**System Owner:** The System Owner is the person responsible for operation and maintenance of a Company IT system.  With respect to IT security, the System Owner’s responsibilities include establishing security awareness and training capabilities that ensure that all IT System Users receive training appropriate to their role, maintaining compliance with Company and state security policies and standards in all IT system activities, and maintaining compliance with requirements for the handling of data processed by the system.

**III. POLICY STATEMENT**

Information and related systems maintained by the Company centrally and within departments and offices are vital assets that need to be available to employees who have a legitimate need for them, consistent with the Company’s responsibility to preserve and protect such information resources by all appropriate means.

To provide reliable and accurate data to the Company community, information resources must be protected from natural and human hazards. Policies and practices must be established to ensure that risks are eliminated or mitigated using best practices validated by security professionals. Employees accessing data must observe requirements for confidentiality and privacy, must comply with protection and control procedures, and must accurately present the data in any use.

The function of this policy is to enhance and help define the policies and procedures of an IT security program to protect Company IT systems and data from credible threats, whether internal or external, deliberate or accidental.

It is the policy of the Company to use all reasonable IT security control measures to:

1. Protect Company information resources against unauthorized access and use;

2. Maintain the integrity of Company data;

3. Ensure Company data residing on any IT system is available when needed; and

4. Comply with the appropriate federal, state and other legislative, regulatory and industry requirements

Protecting information resources includes:

* Physical protection of information processing facilities and equipment
* Assurance that application and data integrity are maintained
* Assurance that information systems perform their critical functions correctly, in a timely manner, and under adequate controls
* Protection against unauthorized access to protected data through logical access controls
* Protection against unauthorized disclosure of information
* Assurance that systems continue to be available for reliable and critical information
* Assurance that the security and forensic needs of the Company are met

Additionally, information entered, processed, stored, generated, or disseminated by information systems must be protected from internal data or programming errors and from misuse by individuals inside or outside the Company. Specifically, the information must be protected from unauthorized or accidental penetration, modification, destruction, or disclosure. Proper account management procedures, security monitoring, and logging practices are required to provide this type of protection of data.

The following principles are the main components of the security policy for physical and logical access that itemizes the standards to which all Company information systems and applications must adhere.

1. All Company systems and their applications will be classified by the Company’s Information Security Officer or designee according to their sensitivity with respect to data confidentiality, system availability, and data integrity.
2. Once classified, the system’s or the application’s minimum authentication and authorization requirements must be determined by the System Owner and documented according to risk and sensitivity.
3. All systems and applications will have documented policies and procedures for:

 a. approving and terminating access

b. obtaining and disabling temporary accounts

c. consistent periodic review and assessment of all accounts for continued needs with documentation as evidence of the review

d. locking accounts after a period of inactivity, with the period of time appropriate to the sensitivity of the system and associated risks

e. logging configurations and review

The organization responsible for an information system is responsible for the prompt deactivation or disabling of accounts when necessary including but not limited to accounts subject to the following circumstances:

* the accounts for terminated individuals shall be removed/disabled/revoked from any computing system at the end of the individual’s employment or when continued access is no longer required
* the accounts of transferred individuals may require removal/disabling to ensure changes in access privileges are appropriate to the change in job function or location
* the accounts for employees who are not working due to any sort of leave, disability or other authorized purpose, or when continued access is no longer required, shall be temporarily disabled for a period consistent with the employee’s personal usage needs and duration of absence
* the accounts for employees suspended for more than one day for disciplinary reasons shall be disabled
1. There will be no anonymous “guest” accounts on any system classified as sensitive. The organization responsible for an information system shall issue a unique account to each individual authorized to access that information resource.
2. Accounts on all systems will use non-shared, unique passwords.  In the instances when systems classified as sensitive must use a shared account in order to do business, strong mitigating controls must be documented and practiced.  In these unique situations, the proposed controls can be reviewed by the Information Security Officer. Those systems residing on a guest network are exempt from this requirement.
3. Physical and logical access to any system will be granted based on least privilege. When establishing accounts, standard security principles of “least privilege” to perform a function must always be used, where administratively feasible. Access privileges should be limited to those that the user has a genuine need for to complete job responsibilities and functions. For example, a root or administrative privileged account must not be used when a non-privileged account will do.  Privileges must never be granted “in case” a user might need them.
4. Access security designs for all systems will be group or role based and privileges assigned to groups or roles will be based on least privilege.
5. Access privileges granted to each individual user will adhere to the principles of separation of duties. Technical or administrative users, such as programmers, System Administrators, Data Base Administrators, security administrators of systems and applications must have an additional, separate end-user account to access the system as an end-user to conduct their personal business.
6. Passwords or PINs are required on all Company issued mobile devices such as tablets, PDAs, and Smartphones.
7. No passwords for any system may be stored or transmitted in clear text.

To provide for the security and forensic needs of the Company, all servers not administered by central Information Technology Unit (ITU) must follow these logging standards. These standards do not apply to workstations. Exceptions to these standards must be evaluated and approved by the IT Security Office.

1. At the unit or department level, a program for documenting and implementing information security monitoring and logging practices must be put in place.

2. At the unit or department level

a. A person in a responsible position needs to be assigned the responsibility of developing and implementing information security logging capabilities

b. The person in this role must develop and implement detailed procedures for reviewing and administering the logs

3. Logging must be enabled to include at a minimum:

a. The event

b. The user ID associated with the event

c. The time the event occurred

4. IT system event logs must be routinely monitored in real time:

a. Log review must include the ability to correlate log information with other automated tools

b. The solution must be able to identify suspicious activities

c. The solution must provide for alert notification

5. The process for responding to malicious events and type of action to be taken must be documented.

6. Prohibit Keystroke loggers from being installed or any other unauthorized monitoring from taking place.

**IV.** **RESPONSIBILITIES**

Vice presidents, department heads and their staffs are responsible for the security, confidentiality, availability and integrity of data and systems to the extent that they have access and or access control.

This policy also places responsibility on department heads and directors to encourage appropriate computer use, ensure compliance with information technology policies and standards by people and services under their control, and implement and monitor additional procedures as necessary to provide appropriate security of information resources within their area of responsibility.

Departments and administrative offices shall develop, manage and review local operating policies and procedures to create the proper security practices for the logical and physical security of information resources.

The Information Technology Unit (ITU) is responsible for establishing and maintaining the physical security of the central computing facilities, including shared file servers managed by ITU, the Company’s communications network, and data for which the ITU is the custodian. ITU will maintain access to centrally-managed computing systems, the campus network, and fileservers managed by ITU.

All users of Company information technology resources are required to adhere to detailed requirements included in the Responsible Use of Computing Policy as well as other Company policies related to the security of information technology resources.

**V. COMPLIANCE**

System owners must have documented procedures for access control and must be able to produce the documented procedures when required for auditing purposes. Evidence of account approval, termination, and disabling must be available when required for auditing purposes.

Failure to honor the requirements set forth in this policy may result in disciplinary or administrative action.

**VI. DESTRUCTION**

Some information stored on the Company’s networks is subject to state or federal data destruction laws. As such, any such protected information will be destroyed pursuant to any applicable law and the Company’s destruction policies.

**VII. EFFECTIVE DATE AND APPROVAL**

This policy shall be reviewed and revised, if necessary, annually to become effective at the beginning of the Company’s fiscal year, unless otherwise noted.