|  |  |  |
| --- | --- | --- |
| Document ID  ITSD106 | Title  IT ACCESS CONTROL | Print Date  **mm/dd/yyyy** |
| Revision  **0.0** | Prepared By  **Preparer’s Name / Title** | Date Prepared  **mm/dd/yyyy** |
| Effective Date  **mm/dd/yyyy** | Reviewed By  **Reviewer’s Name / Title** | Date Reviewed  **mm/dd/yyyy** |
|  | Approved By  **Final Approver’s Name / Title** | Date Approved  **mm/dd/yyyy** |

**Policy:** The Company shall control access to its information to help ensure its confidentiality and integrity.

**Purpose:** To prevent unauthorized access to or use of Company information, to ensure its security, integrity, and availability to appropriate parties.

**Scope:** This applies to all Company information and to all storage and access methods.

**Responsibilities:**

The Human Resources Manager is responsible for reviewing requirements for access (with Information Technology Managers) and Access Control Plan user training.

Information Technology Managers are responsible for reviewing access requirements, convening the Security Review Committee to review the Plan, and verifying updates to the Plan.

The Information Technology Security Manager is responsible for developing an Access Control Plan, presenting the Plan to the Security Review Committee for review, communicating the Plan to Human Resources, monitoring the Plan, revising the Plan, as needed, and enforcing the Plan.

The Security Review Committee is responsible for reviewing and approving the Plan.

Users are responsible for knowing and following the Plan.

**Definitions:** Access control – Enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access (or, providing access to authorized users while denying access to unauthorized users).

**Procedure:**

1.0 planning it ACCESS CONTROL

1.1 Information Technology Managers shall, with the assistance of the Human Resources Manager, determine and evaluate the Company’s position requirements for information access.

1.2 The Information Technology Security Manager shall determine the Company’s current state of access control, to develop a baseline for the Access Control Plan.

1.3 Based on findings related to 1.1 and 1.2, the Information Technology Security Manager shall develop an Access Control Plan and submit it to Information Technology Managers for review and possible revision.

1.4 Information Technology Managers shall convene the Security Review Committee (see ITSD102 IT SECURITY PLAN) for review and final approval of the Access Control Plan.

1.5 The Information Technology Security Manager shall communicate the Plan to the HR Manager, who shall be responsible for training users on the Plan.

**2.0 IT ACCESS CONTROL PLAN**

2.1 The Access Control Plan shall contain the following, at a minimum:

* Business requirements for access regulation;
* Rules for managing user access;
* User responsibility guidelines;
* Access control and operating systems;
* Access control and applications; and
* Monitoring user access.

2.2 The Information Technology Security Manager shall be responsible for enforcing the Access Control Plan.

**3.0 IT ACCESS CONTROL PLAN REVIEW**

3.1 The Information Technology Security Manager shall monitor the Plan (are systems, databases, etc., being used appropriately by the right people) by reviewing access logs, security logs, etc., on a periodic basis (once a week is recommended). Findings of such reviews shall be reported to the Security Review Committee for its review and possible action.

3.2 The Security Review Committee shall periodically (annually, at a minimum) review the Access Control Plan for usability and applicability to Company and legal/regulatory requirements.

3.3 The SRC shall periodically (once every two years, at a minimum) authorize a third-party review of the Plan, to verify its conformance with requirements and to help evaluate the Plan’s effectiveness.

3.4 Based on any findings, the Information Technology Security Manager may be required to revise the Plan. Any revision of the Plan shall be submitted to the Security Review Committee for its review and approval.

**4.0 IT ACCESS CONTROL PLAN UPDATE**

4.1 After any revision of the Access Control Plan, the Information Technology Security Manager shall implement required updates and communicate the revised Plan to the HR Manager. The HR Manager shall be responsible for instructing employees on the revised Plan.

4.2 Within ten business days of any update to the Access Control Plan, Information Technology Managers shall verify that the update has been implemented and is providing the desired results.

**Forms:**

* ITSD106-1 IT ACCESS CONTROL PLAN
* ITSD106-2 IT USER ACCESS CONTROL DATABASE
* ITSD106-3 ACCESS CONTROL LOG
* ITSD106-4 USER ACCOUNT CONVENTIONS

**References:**

**A. ISO 27002:2013 – INFORMATION TECHNOLOGY – CODE OF PRACTICE FOR INFORMATION SECURITY CONTROL**

For more, see <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297>.

**B. IEEE 802.1X – PORT-BASED NETWORK ACCESS CONTROL STANDARD**

This IEEE standard is designed to enhance security of wireless local area networks on the IEEE 802.11 standard. 802.1x provides an authentication framework for wireless LANs which allows a user to be authenticated by a central authority.

**C. GUIDE TO NIST INFORMATION SECURITY DOCUMENTS**

This guide lists a number of NIST documents dealing with the subject of access control. See <http://csrc.nist.gov/publications/CSD_DocsGuide.pdf>.

**Additional Resources:**

A. Create Security Policies with Extended Port Access Control Lists for Windows Server 2012 R2 – <http://technet.microsoft.com/en-us/library/dn375962.aspx>.

**Revision History:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Description of Changes** | **Requested By** |
| 0 | mm/dd/yyyy | Initial Release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**ITSD106-1 IT ACCESS CONTROL PLAN**

1. **Business Requirements For Regulating Access**
2. Every Information Technology user shall have a unique identifier and a system password assigned. See ITSD106-4 USER ACCOUNT CONVENTIONS for guidance.
3. There shall be a system in place for authenticating and authorizing users beyond the login point. Access to applications, databases, etc., once a person is in the system must be controlled.
4. Each user shall be given access to Information Technology resources based on position and department. Users shall be given the fewest privileges needed to perform their duties, as spelled out in their job descriptions.
5. User activity shall be monitored frequently and reviewed for unusual, unauthorized, or illegal activity; current periods of inactivity, etc.
6. User access may be suspended for:

* A number of consecutive failed logon attempts;
* Unauthorized or illegal activity; or
* An extended period of account inactivity.

Account suspension shall be conducted in accordance with ITSD110 Information Technology INCIDENT HANDLING.

1. All users shall be made aware of access control policy and procedures. Users shall sign a statement to that effect and a record of that statement shall be kept by the Human Resources Department.

* All users shall review access control policy on an annual basis and shall sign a statement to the effect that they have reviewed the policy.

1. **Management Of User Access**
   1. Users shall be formally registered at the time of their employment with the Company. Users shall be reregistered upon changing jobs within the company and deleted/unregistered upon leaving the Company or after a specific period (e.g., 30 days) of inactivity.
   2. Access to Company information shall be granted on a need-to-know basis. Users shall be authorized according to minimum access requirements for their duties. Access may be “read only”, “read/write”, or “full access” and users may or may not be given administrative privileges for their computers and for certain data.
   3. Password Control – also see ITSD106-4 USER ACCOUNT CONVENTIONS.
   * Passwords must be eight characters or more in length.
   * Passwords must contain a combination of alphabetic, numeric, and/or special characters.

* Default passwords must be changed upon initial login.
* Users shall change their passwords at least every sixty days. If a user password has not been changed in that time, a password change shall be forced on the user and the user shall be notified of the default password to be used at the next login.
* Passwords shall not be reused consecutively. There should be a system in place to keep a password history and prevent password reuse for several cycles (four or more is recommended).
  + Accounts shall be automatically suspended upon three consecutive failed logon attempts. Users shall apply to the Information Technology Security Manager for a password reset.
  + Systems shall identify and authenticate users before granting access.
  1. The Information Technology Security Manager shall review all users’ access rights/privileges on a regular basis (every 90 days, at a minimum).

1. **User Responsibilities**
   1. Users must secure their equipment if it is to be unattended for any length of time. Screen locks should automatically activate after 15 minutes of inactivity (users may set screen locks to activate sooner and they should be allowed to activate screen locks immediately, if desired).
   2. Users shall have direct access only to services and information that they have been specifically authorized to use. Unless expressly authorized, access to all resources and services is denied. The Information Technology Security Manager shall maintain an access control database for that purpose – see ITSD106-2 USER ACCESS CONTROL DATABASE for guidance.
   3. All communications to external (i.e., Internet-based) resources by way of the Company Information Technology network shall be restricted to authorized users. Users shall apply for permission to access external resources and access shall be authorized on a case-by-case basis.
2. **Operating Systems Access Control**
   1. Access to operating systems shall be limited to trusted, authorized users (for example, Tech Support staff).
   2. Only authorized support personnel shall be authorized to access operating systems and utilities outside of normal business hours.
   3. Access to operating systems and related utilities shall be logged and such logs shall be reviewed periodically (weekly, at a minimum) by the Information Technology Security Manager, who shall report unusual or suspect activity to Information Technology Managers.
   4. Operating systems connections shall be terminated after 15 minutes of inactivity.
3. **Application Access Control**
   1. Access to applications shall be limited to authorized users.
   2. Access to applications shall be limited to normal business hours, with reasonable exceptions.
   3. Application access shall be logged and those logs shall be reviewed by Information Technology Department Managers whose departments are responsible for developing, installing, and maintaining the applications.
   4. Connections to applications should be terminated after a predetermined period of inactivity (15 minutes).
4. **Monitoring System Access/Use**
   1. Instances of access and use of any Information Technology resource shall be automatically logged. ITSD106-3 ACCESS CONTROL LOG may be used for guidance.
   2. Access control logs shall be retained in accordance with legal and regulatory requirements.
   3. The Information Technology Security Manager shall periodically (once a week is recommended) review access control logs and present a status report to Information Technology Managers.

[This page intentionally left blank]

**ITSD106-2 IT USER ACCESS CONTROL DATABASE**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **User ID** | **User Name** | **Department** | **Position** | **Password** | **Password Start Date** | **Resource 1** | **Access privilege** | **Resource 2** | **Access privilege** | **Resource 3** | **Access privilege** |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

[This page intentionally left blank]

**ITSD106-3 ACCESS CONTROL LOG**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Access Date** | **Access Logon  Time** | **Access Logoff  Time** | **Equipment ID and Location** | **Access accepted-rejected** | **Data modification accepted-rejected** | **Nature of activity** |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

[This page intentionally left blank]

**ITSD106-4 USER ACCOUNT CONVENTIONS**

### 1.0 User Naming Conventions

Each Company employee granted access to the Information Technology network shall be assigned a unique user name or user ID. All user account names should be composed of eight or more alphanumeric characters and must follow a consistently applied pattern (for example, the first seven letters of the user’s last name and first initial). Where users may share a pattern (for example, Ben and Bonnie Franklin), a character or number shall be substituted at the end of the second occurrence, to ensure that no two users have the same user name.

### 2.0 User Passwords

User passwords shall be a minimum of 6 alphanumeric characters. Passwords shall be set to expire every 90 days; users who wish to change their passwords more often shall not be prevented from doing so.

Users shall not continuously use the same password. The security subsystem of the network operating system or mainframe system shall be configured to remember at least the last five passwords.

When a new user account is created, the Information Technology Security Manager shall assign a temporary password. Security systems shall be set to force the new user to change his/her password upon logging in for the first time.

### 3.0 User Account Expirations

The Company corporate enterprise network supports a wide range of users. One user type is “Company employee.” Employee user accounts shall not have an expiration date.

Users requiring temporary access, such as consultants or contractors whose tenure is finite, shall have an expiration date on their accounts. Extensions to temporary user accounts shall be coordinated with the departmental Systems Administrator and the HR Administrator.

### 4.0 Home Directories

Each user shall be assigned a home directory on a file server within their department. User home directory names shall be the same as the user name. The user home directory shall have security permissions that allow the both the user and System Administrators full control over all contents in their home directories.

### 5.0 User Group Assignments

The access to resources on the network will be strictly limited to only those users with a specific business need. Security of specific file storage directories on network file servers will be managed by assigning appropriate access privileges to specific user groups. User groups are an administrative collection of users.

Users will be added to groups based on a number of criteria. Each department shall have an associated user group. Within each department, there may be any number of project specific user groups. Users may be members of multiple groups depending on their role in the Company and need for access to company resources. Users may also be members of groups within other departments if there is a specific business need.

**6.0 Workstation Restrictions**

In a high-security network where sensitive data is stored on a local computer, restrict which users can log on from that computer. For example, allow “UserA” to log onto the network only from a computer named “Computer1”.

**7.0 User Profiles**

A user’s computing environment is determined primarily by the user profile. Windows security, for example, requires a user profile for each account that has access to the system. The user profile contains all user-definable settings for the work environment of a computer running Windows, including display, regional, mouse, and sounds settings, and network and printer connections.

A user profile may be customized to restrict what users see in their interface and what tools they have available to use when they log on. For example, an administrator can remove the Administrative Tools folder to prevent a user from changing a configuration.