SOP # _____ Revision:_____
Effective Date:_____

Prepared by:_____
Approved by:_____

Title: **ITSD106 – IT ACCESS CONTROL**

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 IT Management) and Access Control Plan user training.

IT Management is responsible for reviewing access requirements, convening the Security Review Committee to review the Plan, and verifying updates to the Plan.

The IT 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 IT Management shall, with the assistance of the Human Resources Manager, determine and evaluate the Company's position requirements for information access.

1.2 The IT 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 IT Security Manager shall develop an Access Control Plan and submit it to IT Management for review and possible revision.

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

1.5 The IT 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 IT Security Manager shall be responsible for enforcing the Access Control Plan.

3.0 IT ACCESS CONTROL PLAN REVIEW

3.1 The IT 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 IT 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 IT 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 (10) business days of any update to the Access Control Plan, IT Management shall verify that the update has been implemented and is providing the desired results.

Additional Resources:

A. Microsoft's "Overview of Access Control", found at http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/Default.asp?url=/resources/documentation/Windows/XP/all/reskit/en-us/prdd_sec_gyqt.asp.

B. Australian Government Department of Defence, Defence Signals Directorate - Information System Review Checklist, 2005. (http://www.dsd.gov.au/library/pdfdocs/Information_System_Review_Checklist_V3.1.pdf)

References:

A. ISO 17799:2005 – INFORMATION TECHNOLOGY – CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT, CLAUSE 9 (ACCESS CONTROL)

This ISO Standard is designed to provide a comprehensive set of controls comprising best practices in information security.

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. IEEE SPECIAL PUBLICATION 802.12 – AN INTRODUCTION TO COMPUTER SECURITY-THE NIST HANDBOOK

Chapter Ten of this publication deals with personnel and user issues. Sections 10.1.1 (position definition) and 10.1.2 (position sensitivity) mention a couple of important access control issues, least privilege and position duties. The publication recommends that users be granted only the minimum accesses they need to perform their official duties, and that knowledge of the duties and access levels that a particular position will require is necessary for determining the sensitivity of the position.

To see the publication in detail, visit http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/index.html.

ITSD106-1 – IT ACCESS CONTROL PLAN

1.0 Business Requirements For Regulating Access

a. Every IT user shall have a unique identifier and a system password assigned. See ITSD106-4 – USER ACCOUNT CONVENTIONS for guidance.

b. 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.

c. Each user shall be given access to IT 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.

d. User activity shall be monitored frequently and reviewed for unusual, unauthorized, or illegal activity; current periods of inactivity, etc.

e. 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 – IT INCIDENT HANDLING.

f. 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.

2.0 Management Of User Access

2.1 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 (30 days, for example) of inactivity.

2.2 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.

2.3 Password Control – also see ITSD106-4 – USER ACCOUNT CONVENTIONS.

- Passwords must be eight (8) 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 (60) 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 (3) consecutive failed logon attempts. Users shall apply to the IT Security Manager for a password reset.
- Systems shall identify and authenticate users before granting access.

2.4 The IT Security Manager shall review all users' access rights/privileges on a regular basis (every 90 days, at a minimum).

3.0 User Responsibilities

3.1 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).

3.2 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 IT Security Manager shall maintain an access control database for that purpose – see ITSD106-2 – USER ACCESS CONTROL DATABASE for guidance.

3.3 All communications to external (i.e., Internet-based) resources by way of the Company IT 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.

4.0 Operating Systems Access Control

4.1 Access to operating systems shall be limited to trusted, authorized users (for example, Tech Support staff).

4.2 Only authorized support personnel shall be authorized to access operating systems and utilities outside of normal business hours.

4.3 Access to operating systems and related utilities shall be logged and such logs shall be reviewed periodically (weekly, at a minimum) by the IT Security Manager, who shall report unusual or suspect activity to IT Management.

4.4 Operating systems connections shall be terminated after 15 minutes of inactivity.

5.0 Application Access Control

5.1 Access to applications shall be limited to authorized users.

5.2 Access to applications shall be limited to normal business hours, with reasonable exceptions.

5.3 Application access shall be logged and those logs shall be reviewed by IT Department Managers whose departments are responsible for developing, installing, and maintaining the applications.

5.4 Connections to applications should be terminated after a predetermined period of inactivity (15 minutes).

6.0 Monitoring System Access/Use

6.1 Instances of access and use of any IT resource shall be automatically logged. ITSD106-3 – ACCESS CONTROL LOG may be used for guidance.

6.2 Access control logs shall be retained in accordance with legal and regulatory requirements.

6.3 The IT Security Manager shall periodically (once a week is recommended) review access control logs and present a status report to IT Management.