

Table of Contents

1	OVERVIEW	1
2	CONFIDENTIALITY	2
2.1.	CONFIDENTIALITY GOALS	2
2.2.	CONFIDENTIALITY REQUIREMENTS	2
3	ACCESS CONTROL	4
3.1.	ACCESS CONTROL GOALS.....	4
3.2.	ACCESS CONTROL REQUIREMENTS.....	4
4	IDENTIFICATION	5
4.1.	IDENTIFICATION GOALS	5
4.2.	IDENTIFICATION REQUIREMENTS	5
5	AUTHENTICATION.....	7
5.1.	AUTHENTICATION GOALS.....	7
5.2.	PASSWORD REQUIREMENTS.....	7
5.3.	DIGITAL TOKEN REQUIREMENTS	8
6	MONITORING	9
6.1.	MONITORING GOALS.....	9
6.2.	MONITORING REQUIREMENTS	9
6.2.1.	<i>Audit Trail</i>	9
6.2.2.	<i>Log Activity</i>	10
6.2.3.	<i>Log Integrity</i>	10
6.2.4.	<i>Log Review</i>	11
7	MEDIA PROTECTION	12
7.1.	MEDIA HANDLING AND MEDIA ACCESS CONTROLS	12
7.2.	SENSITIVE INFORMATION RELEASE AND MOVEMENT.....	12
7.3.	RECORD RETENTION AND DESTRUCTION OF MEDIA	13
8	PHYSICAL SECURITY.....	14
8.1.	BUILDING PHYSICAL ACCESS CONTROL.....	14
8.2.	DATA CENTER AND SECURE AREA PHYSICAL CONTROLS	14
8.3.	SELECTED VENDOR ACCESS.....	15
8.4.	NON-SECURED AREAS.....	15
8.5.	ACCESS DEACTIVATION.....	15
9	INTERNET	16
9.1.	SCOPE	16
9.2.	INFORMATION MOVEMENT.....	16
9.3.	ACCESS CONTROL	16
9.4.	PERIODIC REVIEW OF AUTHORIZED ACCOUNTS	17
9.5.	AUDIT AND ACCOUNTABILITY OF INTERNET CONNECTIONS	17
10	FIREWALLS AND RELATED SERVICES	18
11	NETWORK SECURITY	19
11.1.	NETWORK ARCHITECTURE	19

11.2.	PHYSICAL SECURITY	19
11.3.	ENVIRONMENTAL CONTROLS	19
11.4.	CHANGE ADMINISTRATION.....	19
11.5.	INTERNAL INTERCONNECTION CONTROLS	19
11.6.	EXTERNAL INTERCONNECTION CONTROLS	20
11.7.	NETWORK DEVICE CONTROLS	20
11.8.	RESTRICTED USE OF DIAGNOSTIC HARDWARE AND SOFTWARE	21
12	REMOTE ACCESS CONTROL.....	22
12.1.	GENERAL CONTROLS	22
12.2.	STANDARDS DESCRIPTION	22
12.3.	APPROVAL AND REGISTRATION OF DIAL-UP/REMOTE ACCESS	22
12.4.	DIAL-UP ACCESS TO LOCAL AREA NETWORKS	23
12.5.	DIAL-UP ACCESS TO WORKSTATIONS	23
12.6.	DIAL-UP ACCESS TO DIAGNOSTIC OR MAINTENANCE PORTS.....	23
12.7.	REMOTE ACCESS VIA EXTERNAL NETWORKS	23
12.8.	REMOTE ACCESS AUTHENTICATION METHODS	24
13	ENCRYPTION.....	25
13.1.	ENCRYPTION/DIGITAL SIGNATURES	25
13.2.	KEY MANAGEMENT	25
13.2.1.	<i>Transport</i>	26
13.2.2.	<i>Storage</i>	27
13.2.3.	<i>Logging</i>	27
13.2.4.	<i>Key Compromise</i>	27
13.3.	DATA RECOVERY	27
14	COMPUTER VIRUSES	29
14.1.	OUTSIDE SERVICE PROVIDERS.....	29
14.2.	ANTI-VIRUS SOFTWARE	29
14.3.	VIRUS SCANNING.....	29
14.4.	SOFTWARE OVERSIGHT.....	30
14.4.1.	<i>Software Oversight Team</i>	30
14.4.2.	<i>Oversight Team Responsibilities</i>	30
15	INFORMATION SECURITY INCIDENTS.....	31
15.1.	RESPONSIBILITIES	31
15.2.	STANDARD INCIDENT RESPONSE PROCEDURE	31
15.3.	INCIDENT RESPONSE REQUIREMENTS.....	32
15.4.	ENTERPRISE COMPUTER EMERGENCY RESPONSE TEAM (CERT)	32
15.4.1.	<i>Membership and Meetings</i>	32
15.4.2.	<i>Response Team Responsibilities</i>	33
15.4.3.	<i>Business Unit Responsibilities</i>	33
16	INFORMATION OWNERSHIP AND DATA ACCESS STRATEGY.....	34
16.1.	DATA ACCESS STRATEGY	34
16.2.	DATA ACCESS STRATEGY ROLES AND RESPONSIBILITIES	34
16.3.	DATA ACCESS STRATEGY REQUIREMENTS	36

1 Overview

This Information Security General Standards of Configuration document is designed for use as a guideline for implementing a minimum level of security on all SFA information systems in accordance with Industry best practices. It is designed to provide guidance in applying information security and control mechanisms for systems in which technology specific standards of configuration are not available.

These general standards should be considered during policy creation across all components of SFA.

2 Confidentiality

Confidentiality is the concept of protecting sensitive information assets from improper or unauthorized access.

2.1. Confidentiality Goals

The goals of Confidentiality are to:

- Protect sensitive information from improper or unauthorized access.
- Protect the organization's proprietary information and all customer sensitive information from unlawful or inappropriate disclosure.
- Comply with Federal Regulations

2.2. Confidentiality Requirements

- All information assets must be classified by level of sensitivity in order to determine the level of confidentiality that must be maintained.
- All organizational and customer sensitive information is not to be disclosed without permission from organizational management and/or the impacted customer.
- All sensitive information must be restricted by a strong authentication and identification method.
- All sensitive information must be released on a need-to-know basis only. Only authorized individuals with a documented business need will be authorized to access sensitive information.
- Sensitive information transmitted over an external network must be encrypted using an approved encryption technique.
- All information and communications systems should present banners informing users, senders, and recipients of the legal restrictions inherent with use.

The following is a sample banner for use in transmitting internal and external electronic mail and faxes:

```
"This transmission may contain information that is
privileged, confidential and exempt from disclosure
under applicable law.  If you are not the intended
recipient, you are hereby notified that any disclosure,
copying, distribution, or use of the information
contained herein (including any reliance thereon) is
STRICTLY PROHIBITED.  If you received this transmission
in error, please immediately contact the sender and
destroy the material in its entirety, whether in
electronic or hard copy format.  Thank you." © 2000
<ORGANIZATION NAME>
```

The following sample banner is recommended for use on internal computing systems and is displayed upon logon or network entry:

"This computer system (including all hardware, software, and peripheral equipment) is the property of <ORGANIZATION NAME>. Use of this computer system is for management-approved purposes. <ORGANIZATION NAME> reserves the right to monitor use of the computer system at any time. Use of this computer system constitutes consent to such monitoring. Any unauthorized access, use, or modification of the computer system can result in disciplinary action, civil liability, or criminal penalties. Please refer to the <ORGANIZATION NAME>'s Information Security Policy for more information."

The following sample banner is recommended for use on external computing systems and should be displayed upon logon:

"Use of this system is intended for authorized personnel only. ALL Individuals using this computer system are subject to having ALL activities monitored and recorded by information security personnel. Monitoring within this system is NOT limited to unauthorized users only. Authorized personnel are subject to monitoring.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, information security personnel may provide the evidence of such monitoring to law enforcement officials.

Inappropriate system use may result in penalties up to and including termination of employment and/or contractual relationships, in addition to other legal remedies."

3 Access Control

Access Control is the process of limiting access to system resources only to authorized users, programs, processes, or other network systems.

3.1. Access Control Goals

The goals of Access Control are to:

- Permit access to information resources only to authorized users with a need-to-know in order to support the requirements of an assigned job function.
- Ensure that unauthorized users are prevented from gaining access to information resources.

3.2. Access Control Requirements

- Management of the responsible organizational unit must authorize access to information resources, both logical and physical.
- Access to information and technology must be on a need-to-know basis. Users must be limited to the minimum permissions and privileges needed to perform the business-specific function or transaction.
- Organizational Unit management or Human Resources will notify Information Security personnel upon transfer, change of responsibility, leave of absence, or termination of a system user. (Information Security should make a User-Status Change Form available. This form should be submitted to Information Security immediately upon occurrence of such an event.)
- Physical access to information systems assets must be restricted to persons with a business purpose only. Physical hardware and software must be protected from unauthorized access.
- Newly created resource objects must not default to public access and must be limited to the creator or pre-defined subset of users.
- Access control mechanisms must be utilized to permit granular restrictions at the file, record, field, or functional level.

4 Identification

Identification is the process of uniquely distinguishing the uniqueness of a system user in order to establish accountability.

4.1. Identification Goals

The goals of Identification are to:

- Establish the identity of a user.
- Provide unique accountability for the actions that user performs.

4.2. Identification Requirements

- Each employee will have a unique ID, which should be identical across all authorized system resource.
- Each user ID should comply with an established name construction standard.
- Each user ID must be assigned to only one person.
- Each user must be identified and authenticated prior to performing any actions on the system.
- Shared user ID's are prohibited by default. If a shared user ID is justified, an individual accountability mechanism must be employed (such as su). Information Security must approve and document the use of shared user IDs.
- The date and time of the last successful login or the number of unsuccessful login attempts since the last successful login must be displayed to the user after successful completion of the Identification and Authentication process.
- Any User ID performing three unsuccessful login attempts during a one-hour period should be disabled. The user must contact a System Administrator or designated Help-Desk in order to verify identity and reactivate the account.
- Identification and Authentication must be completely processed by the systems prior to displaying the failed attempt indicator. All failed login messages shall be non-descriptive (e.g. the message will not indicate what part of the log-in failed).
- Only the approved systems support group can reset a disabled user ID or automatic password generator, based upon Information Security standard alternate authentication procedures.
- Users employing a public network to access information assets from a remote location (e.g. dial-up, Internet, LAN, WAN or other method) must use an Identification and Authorization method that has been approved by Information Security. In the case of system access via the Internet, a Virtual Private Network (VPN) is recommended.
- Any user ID that has been inactive for a period of 90 days or more will be disabled. If a request for reactivation of the account is not received in 90 days, the account and all associate data will be deleted.

- An approved warning banner should appear on all screens prior to displaying any organizational logos or banners, and before initiating the Identification and Authorization process. Refer to section 2.1 for approved warning banners.
- All user-ID's and default accounts included with an off-the-shelf product must be renamed if possible and the default password changed. Privileged vendor supplied ID's must be documented and controlled by Information Security.
- All system resources should have a session termination capability enabled after a maximum of 15 minutes of inactivity. Upon session-end, the system should clear any session information from the screen and require the user to re-authenticate prior to allowing access to viewing the screen data or accessing the system.

5 Authentication

Authentication is the process of verifying the identity of a user. This can be accomplished by determining:

- Something a user *knows* such as a password or a PIN;
- Something a user *has* such as password-generating token;
- Something that *is* the user, such as a fingerprint or retinal pattern; and/or
- A combination of the above.

5.1. Authentication Goals

The goal of Authentication is to verify that a system user is who they claim to be.

5.2. Password Requirements

- Authentication information, (e.g. password, PIN, or token), must never be disclosed or shared.
- New user ID's must be assigned pre-expired passwords that force the user to change upon first use.
- Initial passwords should randomly generated.
- The current user password must not be maintained in any intelligible format within a system file or registry. If a user forgets his/her password, physical identity should be verified and only a new pre-expired password assigned forcing the user to change upon successful login.
- Passwords must not be written down. Passwords that are written down must be changed immediately and the documentation destroyed.
- The display or printing of Passwords must be masked, suppressed, or otherwise obscured such that it will not be viewable by anyone after issuance.
- Passwords must be changed at an interval not to exceed 90 days. (Some passwords may require more frequent changes based on the information being secured and management direction.).
- A password history file must exist and prevent the reuse of the previous five (minimum) passwords chosen by the user.
- A minimum password age of 1 day should be required to prevent users from consecutively changing their password, clearing the previous password from history records and allowing its reuse.
- Passwords and other authentication information (PINs, keys, etc.) must be encrypted.
- Passwords should be at minimum, six characters with at least one alphabetic and one numeric character preventing easily guessable combinations.

- User passwords must not be scripted, such as use within an auto-login, function key, macro, or other method.
- Recommended Password Guidelines:
 - □ Passwords must not be the same as the user ID.
 - □ Passwords should not be easily guessable, and therefore the user should be recommended to avoid passwords such as:
 - Proper names such as family members, pets cities;
 - Numbers, such as telephone, social security or license plate numbers;
 - Activities associated with the user, such as a sports team, hobbies, cars, etc.;
 - Words related to the organization such as department names, site names, financial terms, etc.;
 - Generally used words, such as dictionary words, common slang, terms, etc.
- Any time that a user with access to a privileged account (such as root or administrator accounts allowing elevated permissions) leaves the organization or changes job duties; passwords for that account should be changed immediately.
- Password change capabilities should be available to the user at any time they believe an account password may have been compromised. All users should be advised that in such a case they suspect a password compromise, their actions should include immediately changing the password and notifying Information Security.

5.3. Digital Token Requirements

The following applies for all system utilizing digital tokens (“tokens” are electronic one-time password generators):

- A digital token must be unique to a single user.
- Users of Digital tokens must follow the same guidelines for passwords and user IDs. They should not be shared among users.

6 Monitoring

Monitoring is the process of gathering information related to compliance with policies and standards.

6.1. Monitoring Goals

The goals of Monitoring are to:

- Provide for the logging of events.
- Ensure that each event is associated with a particular user.
- Provide a mechanism to retrieve and report information on logged events.
- Report on the effectiveness and compliance to systems security requirements.

6.2. Monitoring Requirements

All organizational entities or individuals that are responsible for installing and maintaining servers, firewalls, routers and gateways within the organization must implement these controls for all configurable systems and devices.

6.2.1. Audit Trail

- Auditing and logging must be performed on production systems and applications where it is available. A risk assessment conducted by organizational unit management will determine the criticality of systems.
- The system must provide an activity log that contains sufficient information for after-the-fact investigation of unauthorized activity or loss.
- Technology custodians and systems administrators are responsible for ensuring that systems are configured in accordance with security standards of configuration and technology.
- High-risk systems at the network perimeter must be monitored with intrusion detection software at both the network and host level, in accordance with Information Security Standards.
- Systems must securely log all significant computer security relevant events. Log entries must provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with Information Security measures. Examples of computer security relevant events include:
 - Successful and unsuccessful session log-ins;
 - Identification and Authentication failures;
 - Security Administration activity;
 - All activities performed by privileged users; and
 - Failed attempts to access information.

- Specific information (at a minimum) must be included in the tracking record associated with each event:
 - □ User ID
 - □ Associated terminal, port, network address, communication device, etc.
 - □ Information or system accessed
 - □ Date and time of access
 - □ Type of event
 - □ Result of event
 - □ Reason for failure
- The identity of the user, or processes acting on behalf of the user, must be maintained for the duration of the session. For example, some programs change mode or privilege during execution. This should not result in the loss of the audit trail or identity of the user.
- Actual or attempted authentication information, e.g., passwords, PINs, and clear-text cryptographic keys must never appear as part of the audit record.
- Commands issued by computer system operators/administrators must be traceable to specific individuals via the use of comprehensive logs.
- Logging of business-specific events, such as updates to financial data, should be performed within the application in accordance to organizational guidelines. A risk assessment should be performed on each application to determine the specific events that should be logged and audited.

6.2.2. Log Activity

- To assure that users are held accountable for their actions on system or network elements, one or more records tracing security relevant activities to specific users must be securely maintained for a minimum of one year. Consideration should be given to any legal requirements mandated by regulatory agencies governing the organization.
- For critical or sensitive applications or resources, logs should be generated for all access, additions, modifications, and deletions whether authorized or unauthorized.
- To deter improper behavior, foster user accountability, and allow expedient systems management, all activities that alter production data must be able to be reconstructed from logs.
- Application and/or database management system software must keep logs of user activities and statistics related to these activities which will allow them to spot and issue alarms reflecting suspicious business events.

6.2.3. Log Integrity

All computers connected to the organization's internal network must have the current time accurately reflected in the internal clock. Automated methods must be used to accurately synchronize these systems.

A log of major security relevant events must be retained for a period of time appropriate for the particular environment or at least one year. These logs are important for error correction, forensic auditing, security breach recovery and related efforts.

The activity log and any associated control mechanisms must be protected from unauthorized access and modification. Mechanisms to detect and record significant computer security events must be resistant to attacks. These attacks include attempts to deactivate, modify, or delete the logging software or the logs themselves.

All logs should be secured and maintained for forensic purposes.

6.2.4. Log Review

Logs detailing the events stated in “Audit Trail” must be generated for and reviewed by the responsible operational area, business unit or Information Security. To allow proper remedial action, the operational area, business unit or Information Security personnel must review records reflecting security relevant events in a periodic and timely manner, at a minimum, once each month.

All WAN access system logs must be maintained in a form that cannot readily be viewed by unauthorized persons. A person is unauthorized if he or she is not a member of the internal audit staff, systems security staff, network management staff, computer operations staff, responsible business unit or if he or she does not have a documented business case for such access.

Any known actual or attempted misuse of, or unauthorized access to organizational computing systems, networks or facilities must be reported to Information Security immediately.

7 Media Protection

This section outlines the security measures for the handling, storage, and access of media containing organizational information. This includes, but is not limited to, hard disks, removable hard disks, Zip disks, floppy disks, tapes, cartridges, microfiche, microfilm, and paper documents.

Organizational units are responsible for ensuring that media security and controls are being maintained. Each organizational unit should perform periodic reviews of their areas to ensure media security controls are in place.

7.1. Media Handling and Media Access Controls

All *Sensitive* information created and used in each department must be properly secured at all times. Under no circumstances will any media be left unattended. Each department must ensure that media is stored in a controlled location where access is limited to people with a business need.

- All electronic and magnetic media must be removed from work areas and secured when unattended.
- *Sensitive* media, including paper documents, will be secured when unattended or not in use.
- *Sensitive* media will be stored in:
 - File rooms with physical security controls approved by the organization's Information Security department and any group with physical security responsibilities;
 - Fireproof file cabinets with physical security controls;
 - Off-site storage approved by Information Security and any group with physical security responsibilities; or
 - Controlled environment media storage areas, such as a data center storage environment.

Confidential information should be contained in organizational facilities with proper physical controls. If *confidential* information is transported outside of organizational facilities, proper care must be taken to ensure that only authorized personnel have access to the media.

7.2. Sensitive Information Release and Movement

- Each department with a responsibility of handling media is also responsible for tracking release, movement, or duplication. Organizational unit management must approve the release of all media.
- The owner of the media or information stored in the media is responsible for its backup and duplication.

- Where appropriate, receiving parties should sign a non-disclosure agreement.
- Media returned from an external location must be checked for virus contamination.

7.3. Record Retention and Destruction of Media

- Media that is retained for organizational record, audit, or regulatory reasons must maintain the proper level of information security as appropriate to the sensitivity of the information contained on the media.
- Retained media may contain information such as:
 - Confidential records or correspondence
 - Access information such as passwords, user IDs
 - Customer information
 - File and system information
- This media must be protected by proper physical and/or logical controls while in retention.
- All information and media not required for retention will be destroyed. The destruction of this media must be in compliance with organizational and regulatory policy and guidelines. An authorized media destruction vendor should perform this function.
- Electronic mail is to be maintained on messaging servers and clients for a period of no longer than 90 days from the date of message receipt, and the messages should not be archived. Variations in such timeframes may be implemented based upon organization or regulatory requirements.

8 Physical Security

This section outlines the security measures for ensuring that physical access to information systems, assets, and media is controlled.

Physical access to information processing and storage areas and their supporting infrastructure (communications, power, and environmental) must be controlled to prevent, detect, and minimize the effects of unauthorized or unintended access to these areas (e.g., unauthorized information access, or disruption of information processing itself).

8.1. Building Physical Access Control

This Standard applies to the implementation of physical access controls for data centers or any secured area related to information system assets, and should comply with standards established by entities or units responsible for overall physical security.

Physical access controls must be in place for the following:

- Data Centers
- Areas containing servers and associated media
- Networking cabinets and wiring closets
- Power and emergency backup equipment
- Operations and control areas

8.2. Data Center and Secure Area Physical Controls

Access permissions to data centers and secured areas will be granted for those employees, contractors, technicians, or vendors who have legitimate business responsibilities in those areas. Authorization will also be based on the frequency of need for access to the area.

Authorization to receive physical access to a restricted area should be granted by both, organizational unit management responsible for the secured area, as well as the unit or entity responsible for overall physical security.

Once an access card has been issued:

- It is intended for the sole use of the person issued the card.
- The practice of “piggy-backing”, (avoiding security by following another person in), to gain access to a secured area is prohibited.
- The cardholder must immediately notify their manager in the event of a lost card.
- Any cardholder who allows a non-cardholder into a secured area must:
 - □ Escort the visitor where possible
 - □ Assume the responsibility for that person’s activities

- Complete the visitor log for the non-cardholder

8.3. Selected Vendor Access

Vendors that perform regular or ongoing work may be permitted to access secured areas without an escort with the responsible manager's approval. These selected vendor technicians will have easily recognized, photo ID cards that permit access to the secured area. Upon conclusion of their assignment, responsible managers should confiscate the ID and return it to the issuing authority.

All vendors are responsible for their activities as well as that of their employees, vendors, or subcontractors.

8.4. Non-secured Areas

Access to offices, cubicle workspaces and the contents of such must be secured where possible. This is the responsibility of the occupant of the workspace.

Sensitive information assets must be secured when not in use and at the end of the workday.

Specifically:

- Offices should be locked
- Filing cabinets locked
- Overhead bins locked
- Media storage (CD's, diskettes, tapes, etc.) placed in a secured area or cabinet
- Paper documents, files, folders, etc. placed in a secured area or cabinet

When office locks are not available, as in the case of cubicles, all computer equipment must be secured when the custodian of these devices is not present. Laptop computers should never be left unsecured outside of work hours or during extended periods away from the work area.

8.5. Access Deactivation

It is the responsibility of the cardholder's manager to forward the access card to the issuing authority upon termination, transfer, or change in status that requires a change in access privileges.

An access card must be deactivated as soon as the transfer or termination is determined. This request must be through written notification from the cardholder's manager.

9 Internet

Access to Internet services and associated information technology resources should be controlled and protected in a manner consistent with general standards of configuration and/or technology specific standards, to preserve the confidentiality, integrity, availability, and accountability of organizational information and resources.

This section defines the recommended standard for providing Internet services at a managed risk level. Failure to adhere to this standard exposes an organization to increased vulnerability to the threats of unauthorized access, theft of information, theft of services, and malicious disruption of services.

9.1. Scope

This section applies to all employees, contractors, vendors, who use the Internet through organizational computing or network resources. All Internet users are expected to be familiar and comply with these practices.

9.2. Information Movement

All information downloaded to organizational computing resources via the Internet must be screened with virus detection software prior to use.

- Users must not place organizational material (software, internal memos, etc.) on any publicly accessible Internet computer, which supports anonymous FTP or similar services, unless management has first approved the posting of these materials.
- Internal organizational information must never be placed in any location, on machines connected to internal networks or on the Internet, unless ALL persons who have access to that location have a legitimate need-to-know and the information has been protected using controls approved by Information Security.

9.3. Access Control

- All users wishing to establish a trusted connection via the Internet with organizational resources must authenticate themselves at the firewall before gaining access to the internal network.
- Users are prohibited from using new or existing Internet connections to establish new business channels, without the joint approval of business unit management and Information Security. These channels include electronic data interchange (EDI) arrangements, electronic malls with on-line shopping, on-line database services, etc.
- All passwords and user IDs must meet organizational password requirements.
- Change control plays a fundamental role in ensuring the security of the Internet connection. To accomplish proper configuration management, Internetworking

infrastructure must be completely documented and maintained, including, but not limited to:

- All hardware devices and components
- All firmware components
- All operating system and application software components
- Version and revision numbers of the above devices and components
- Physical and logical network addresses
- Connecting circuit numbers
- Options enabled at the software level

9.4 Periodic Review of Authorized Accounts

Network administrators should periodically reconfirm the validity of all accounts, electronic mail, and alias authorizations. The period between re-confirmations must not exceed six months. The user authentication account database will be monitored for unusual activity.

9.5 Audit and Accountability of Internet Connections

Information Security will review the Internet connection audit reports created on the firewall for any unusual activities. Alarms must be in place to alert data center personnel and Information Security about security or other related events generated from the firewall. This should be performed with real-time network monitoring tools.

Events to be monitored include:

- Behavior in violation of Information Security Policy and Standards
- A new server attaching to the network
- A new host coming onto the network
- Emergence of a new MAC address on the network
- Host not responding
- Well known attack signatures

10 Firewalls and Related Services

Organizational Internet architecture should be designed to ensure that only authorized users have access to the Internet. In conjunction, the following standards should apply at the firewall(s):

- Alarm or monitoring tools should be used to alert network administrators and Information Security of security related events originating at the firewall.
- All non-essential networking or system services must be eliminated or removed from the firewall.
- The system logs generated from the firewall must be reviewed on a daily basis to detect any unauthorized entry attempts or unusual behavior.
- All unauthorized access through the firewall must be reported to Information Security.
- Strong authentication will be required to access the firewall administrative functions.
- Verify firewall system integrity once every two weeks.
- Networking traffic will be subject to filtering based on current security requirements as determined by Information Security.
- All programming language systems that enable the use of executable code (i.e. Active X, Java, Java script and other active content) should by default be blocked at the firewall. Active content technologies vary in risk level and should be reviewed and assessed on a case-by-case basis by Information Security and organizational unit management prior to being allowed through the firewall. Documentation should be maintained and reference made to the approval within the comments of the firewall rule set.
- Virus protection software will be utilized on all Internet e-mail gateways.

11 Network Security

This section defines the minimum requirements necessary for providing appropriate security controls across a corporate WAN, and any interfaces with external connections such as the Internet, Business Partners, and Service Providers.

11.1. Network Architecture

- The network architecture must allow for redundancy in communication paths to prevent loss of service due to link outages. Additions to the network will follow this strategy.
- The network architecture must be clearly documented to facilitate identification of components during network analysis, change operations and problem investigations. Network administrators are responsible for creating and updating network diagrams. Additions and deletions to existing documentation should be modified in conjunction with change administration procedures. The network administrators should be required to provide this documentation to management as needed without notice.

11.2. Physical Security

Physical security of the network must be maintained in accordance with the organization's established physical access strategy and policies.

11.3. Environmental Controls

- Environmental controls must be in place to protect the security and integrity of the network.
- Access to network system documentation such as network diagrams, routing tables, IP addresses, etc., must be limited to authorized personnel only.
- All networking equipment must be protected against damage from environmental exposures such as water, fire, or natural disaster.

11.4. Change Administration

All changes to the network must be documented in accordance to organizational standards and reported to Information Security.

11.5. Internal Interconnection Controls

- Interconnection of internal wide area, metropolitan, or local area networks should be strictly controlled and monitored. Connectivity must be explicitly authorized by network management personnel, comply with Information Security standards of configuration, and be authorized by Information Security personnel.
- New connection or insertion of all devices must be documented and scheduled.
- Networks will be partitioned into logical domains separating users from host resources.

- All information sent through the network must be traceable. For example, the source originator and the destination recipient must be identified within the datagram.
- Network traffic should be monitored for authorized IP and corresponding MAC addresses. Unauthorized packets should be dropped.
- Connectivity and Access controls must be closely monitored and re-evaluated as the network infrastructure expands and additional services are added.

11.6. External Interconnection Controls

- Information Security must explicitly authorize all new connections to external public networks. If the new connection is an additional connection to a previously certified external connection and the connection is made following the same configuration then no prior approval from Information Security is required.
- Information that would reveal access methods to organizational systems or networks via public switched networks or dial-up, as well as information maintained within such systems, is considered sensitive and must not be disclosed to unauthorized personnel.
- Interconnections must be configured such that, approved identification and authentication procedures are in place to allow only authorized users onto the network.
- Personnel using remote access to organizational networks and systems must be notified of and held subject to specific rules and agreements covering the use of such a service as well as any financial, regulatory, and legislative issues.
- External connectivity will be authenticated cryptographically or through the use of two-factor authentication such as password generators, or other devices approved by Information Security.
- Modem connections should be centrally managed for a single-point-of-entry. Modem users should be authenticated using two-factor strong authentication, such as a token or other approved security device. In the event of legacy systems requiring a direct modem connection, other control mechanisms should be instituted such as direct callback to a known number.

11.7. Network Device Controls

Routers are the primary information communication component within an internetworking environment. Much of the security protection associated with transport of information is provided router configuration, specifically protocol and address filtering.

- Only authorized administrators are allowed to access routers.
- All logical management of network devices must be performed using unique individual authentication and generate unalterable logs to ensure accountability.
- Network devices should be configured to allow only authorized IP addresses to connect. Telnet should be avoided when possible and SSH or Secure-CRT used. If Telnet is the only access available, it should not be used from the Internet unless connected to the network through a VPN tunnel. Telnet is transmitted over the wire in plaintext and authentication credentials are subject to compromise.

- All network device sessions must time out. The maximum acceptable time out period is twenty (20) minutes.
- All remote access entry points should be protected using strong authentication methods. Scanning software is available for telephone networks to allow penetration tests to be performed against remote entry points.
- All network device configuration passwords and Simple Network Management Protocol (SNMP) community strings must follow the ORGANIZATION'S Information Security Policy (i.e. is difficult to guess, minimum length, etc.) in addition to using password encryption.
- SNMP traffic should be restricted to only authorized/trusted devices on the network. Such as HP Openview or other network monitoring and control devices.

11.8 Restricted Use of Diagnostic Hardware and Software

- Diagnostics tools that scan networks for hosts, perform security tests, or capture information are prohibited without the express permission of Information Security.
- Only authorized personnel can use network diagnostic test hardware and software, such as sniffers and monitoring devices to monitor traffic on the ORGANIZATION'S network.
- Although software is readily available to network users via Internet freeware, personnel must be notified of the severity of this restriction. Network-based intrusion detection software will recognize use of scanning software on the network. Such alerts should be investigated immediately and stiff penalties imposed on the culprit.

12 Remote Access Control

This section defines the baseline security controls recommended for remote access to organizational information systems and networks.

12.1. General Controls

- All dial-up users must be properly authorized by management and be authenticated through the use of an approved method. It is recommended that approved mechanisms be a type of strong two-factor authentication such as a password-generating token used in conjunction with a PIN.
- Dial-up entry should be restricted to a centralized point for all users. This concept is analogous to that of single point-of-entry for Internet users accessing resources. Centralized functions allow more efficient manageability, accountability, and audit mechanisms.
- Dial-up directly into all network resources should be prohibited. However, limited instances, such as out-of-band management of routers, will require such access. Strong authentication mechanisms as well as encryption capable modems should be utilized in these cases.
- Dial-up access to directly to internal workstations or servers should be strictly prohibited.

12.2. Standards Description

All dial-up access to organizational networks and computer systems must be protected by an additional security layer such as use of real-time intrusion detection at the protocol level.

12.3. Approval and Registration of Dial-Up/Remote Access

All new procurements or service requests, which have components or services, related to dial-in or remote access must be reviewed and approved by organizational unit management and Information Security. Examples include requests for analog and digital telephone lines, digital-to-analog converters, modems, or remote-control software such as PCAnywhere.

The review and approval process must evaluate:

- Appropriateness of the requested dial-up or remote access application.
- Selection of appropriate dial-up access entry points.
- Levels of acceptable risks and costs in selecting an appropriate dial-up user authentication option.
- Documentation of the requested equipment.
- Tracking of the respective service, software, or equipment.

12.4. Dial-Up Access to Local Area Networks

- Local area networks and other multi-user departmental systems must utilize centralized communication servers or equivalent modem pooling configurations for all dial-up access applications.
- Any approved, non-centralized dial-up access must be authenticated using an authentication method approved by Information Security.
- Individual organizational units, workgroups, or departments should not be permitted to establish dial-up services to their specific resources. They should have easy access to tie centralized functions into their networks
- Telephone line scanning software should be utilized to perform periodic (at least quarterly) scans of the organization's telephone networks to identify and eliminate unauthorized entry points.

12.5. Dial-Up Access to Workstations

- Modems connected to workstations must not be enabled in auto answer mode (permitting in-bound access).
- Any workstation applications requiring only outbound dial-up access to external systems are not required to be equipped with supplemental authentication as long as the analog or digital telephone line is setup for outbound only through a controlled PBX or switch. Any use of the modem will be logged.
- Installation of telecommunications components required for dial-up or remote access must be configured to restrict access to the necessary business needs.
- Remote access and control software such as PCAnywhere, should never be utilized for dial-up based remote access. IP services within such software may be allowed with proper configuration once outside access has been established through a centrally managed entry point

12.6. Dial-Up Access to Diagnostic or Maintenance Ports

Dial-up access connections for diagnostic equipment and maintenance purposes (e.g., front-end communications processor support and network router programming or diagnostics) should use a strong authentication mechanism to control access to information assets. Dial-up access connections must be designed and implemented in a manner that ensures compliance with this standard.

12.7. Remote Access via External Networks

Remote access to organizational computing resources via an external network (e.g. the Internet or third-party Wide Area Network) must adhere to the following standards:

- Broadband access to the network should only be made available via a Virtual Private Network (VPN). VPN access allows all inbound and outbound traffic to be encrypted using IPSEC tunneling across an unrelated network

- The VPN Gateway should be configured so that, traffic from external networks will be authenticated at the firewall using strong authentication;
- External access must be monitored and logged at all times,
- Only organizational approved and distributed client software may be used for remote access to information systems
- Once access to internal networks has been established via the VPN, users may reach internal resources through an approved configuration of remote control software.

12.8 Remote Access Authentication Methods

Dial-up access controls must be implemented only through approved combinations of hardware and software security tools that meet all of the following requirements:

- Unique identification or access code (user ID) for each user.
- Access control software/hardware that protects stored information and the security system from tampering.
- Audit trails of successful and unsuccessful log-on attempts.
- Capability to limit the number of unsuccessful log-on access attempts.
- Appropriate verification of the remote user's identity by approved methods of authentication, using one or more of the following:
 - □ dynamic passwords
 - □ application specific access controls
 - □ closed user groups
 - □ security modems
 - □ fixed passwords

13 Encryption

This section outlines the recommended minimum requirements for the encryption of information assets in the organizational environment. Data encryption standards are determined by regulatory, business partner, and risk management requirements.

Encryption Standards are separate from messaging and communications protocols and standards. The Encryption Standard addresses the preferred encryption algorithms and not the implementation method. Users should contact Information Security for guidance on encryption techniques.

It is recommended that the following organizations and their standards be considered when implementing encryption policies:

- X9 – Committee for Standards
- FIPS – Federal Information Process Standards
- ANSI – American National Standards Institute
- NIST – National Institute for Standards and Technology
- ISO – International Standards Organization

13.1. Encryption/Digital Signatures

- Encryption processes should be reviewed and approved by Information Security before implementation.
- Users agree not to distribute, directly or indirectly, encryption software as defined in United States International Trade in Armaments Regulations (ITAR).
- Any sensitive data that is transmitted across communication networks should have encryption processes implemented.
- Any sensitive data transported in computer-readable storage media (such as magnetic tapes, floppy disks, or CD-ROMs), should be encrypted.
- Encryption regulations should be reviewed as they pertain to the specific industry and a minimum level of encryption established for each business function. Electronic commerce transactions conducted via the Internet should employ a 128-bit level encryption via SSL.

13.2. Key Management

- Information Security is responsible for overseeing the creation, retention, and destruction of all organizational encryption keys. This includes maintaining a current inventory of all encryption keys with description as to their purpose.
- Keys should only be used for a single designated purpose. For example, a PIN-encryption key should not also be used for key encryption, and a key-encryption key should not be used for PIN-encryption.

- Private encryption keys are considered sensitive information, and access to such keys must be strictly limited to those who have a need-to-know. Approval for the release or distribution of encryption keys to employees, consultants, contractors, or other third parties should be the responsibility of senior Information Security management.
- Encryption systems should be designed such that no single person has full access to encryption keys. This can be achieved by separation of duties and dual control. Separation of duties refers to use of more than one individual to handle a certain important activity, while dual control means that two people must be simultaneously present for an important activity to be accomplished.
- Personnel responsible for key management should be under confidentiality agreement and subject to background investigation.
- Persons entrusted with a key component must reasonably protect the component such that no person can observe or otherwise obtain the component.
- Whenever such facilities are commercially available, the organization should employ automated encryption key management processes.
- All encryption keys must have a stated life and must be changed on or before the stated expiration date. Any keys used to encrypt organizational information should expire and require regeneration at a periodic interval not to exceed one year.
- Whenever encryption is used, the keys employed must be generated by means that are not easily replicated by an adversary, and which will yield keys that are difficult-to-guess. An example of this key generation process is the use of a pseudo-random number generator that utilizes the low order bits of the computer clock as a non-repeated variable within the encryption algorithm.
- Whenever user-chosen encryption keys are employed, the encryption system must prevent users from employing keys generated with less than eight (8) characters of variable input.
- Only two approaches for protecting plaintext (readable) master keys are acceptable. Master keys may be manually handled via dual control with split knowledge. Alternatively, they may be stored in tamper-proof modules. In all other places, they must appear only in encrypted form.
- All supplies used for the generation, distribution, and storage of keys (such as photocopies, printer ribbons, and the like) must be protected from disclosure to unauthorized persons. Keys or key components that have been used for cryptographic purposes must be destroyed when no longer required and destruction witnessed and documented by a third party.
- Encryption keys must be protected from unauthorized disclosure via technical controls such as encryption via a non-duplicate key and use of tamper-resistant hardware.

13.2.1. Transport

- If private encryption keys are transmitted over communication lines, they must be encrypted. The encryption of keys should be performed with a stronger algorithm than is used to encrypt other sensitive data protected by encryption.

- If encryption is used, the information protected with encryption must be transmitted over a different communication channel than the keys used to govern the encryption process.
- Clear text key components must be split into at least two parts and transported in separate tamper-evident packaging via separate carriers.
- When bringing keys from the location of generation to the location of loading, the key loading device must be:
 - □ A physically secure Tamper Resistant Security Module.
 - □ Under the supervision of a person authorized by management, or stored in a secure manner such that no unauthorized person may have access to it.
- Key loading devices should not retain clear-text copies of any key it has successfully transferred.

13.2.2. Storage

- If encryption is used to protect sensitive data resident on computer storage media, the encryption keys and related generation components (initialization vectors, time-and-date stamps, salt parameters, etc.) used in the encryption process must not be stored anywhere on this storage media in unencrypted form.
- Keys should only be maintained at locations approved by Information Security.
- If two or more of the key's components are stored within the same security container, then the components should be secured in their own tamper evident packaging to preclude one component holder from gaining access to the other components.

13.2.3. Logging

A record must exist that logs every instance when a container securing cryptographic materials is opened. It should include date, time, persons involved, and purpose of access.

13.2.4. Key Compromise

- Information Security must be notified immediately if a key compromise is suspected or known.
- Keys must be changed if compromise is suspected or known.
- Keys encrypted under or derived from a known-compromised key must be changed.
- Keys must not be changed to a variant or a transformation of the compromised key.
- The amount of time in which the compromised key remains active should be consistent with the risk to affected parties.

13.3. Data Recovery

- All general-purpose encryption processes used within the organization must include data recovery functions. These special functions allow management personnel to recover encrypted information should there be system errors, human errors, or other problems.

- Keys used for digital signatures, digital certificates, and user authentication must never be included in a key escrow arrangement. To make these keys available to third parties allows potential for compromise of process integrity.
- Whenever encryption is used, employees must not delete the sole clear text version of data unless they have first demonstrated that the encryption process is able to reestablish a readable version of the data.
- Whenever encryption is used to protect sensitive data, the relevant owner(s) of the data must explicitly assign responsibility for encryption key management.
- If both encryption and message authentication codes (MACs) are used, separate keys must be used for each.

14 Computer Viruses

This section defines the recommended standards of configuration required for computer virus detection and removal. The intent of anti-virus controls is to prevent or minimize operation disruption and/or loss of data resulting from the introduction of computer viruses as well as reducing the risk and/or exposure of passing infected files to customers and business partners.

A computer virus refers to a computer program or code that is designed to disrupt the operations of computer systems and/or to destroy electronic information. Computer viruses often have the capability of covertly attaching themselves to other programs. Some viruses are specifically programmed to steal information. Computer viruses may be introduced into the environment, accidentally or deliberately, through the use of infected diskettes, download or transfer of files, and/or accessing e-mail attachments.

These standards should be considered for all components of the computing environment, including personal computers, networks, applications, databases and media with a priority given to virus detection processes at high-risk areas of network such as file-transfer and messaging gateways.

14.1. Outside Service Providers

- Outside Service Providers who install or remove software from organizational servers or workstations should be advised of and held accountable to the organization's policies and requirements as they pertain to virus detection and removal.
- Thoroughly scan and test all software before installation on any computing resource.
- A virus prevention clause should be included in all third-party service agreements and contracts.

14.2. Anti-virus Software

Current versions of standard or certified virus protection software should be designated and notification distributed throughout the environment. The current version should be installed on all systems with writeable media. Virus scanning pattern files should be updated as required by release of new release of malicious code or at a minimum, every 30 days.

14.3. Virus Scanning

- Scanning for viruses must be a regular practice. Administrators must ensure continuous, real-time scans of servers and workstations.
- All diskettes or file transfers (no matter the source) must be scanned before being used or before being transferred to workstations or servers.
- Server administrators must also ensure that end users are able to scan their floppy drives, external media, and local hard disks. It is the responsibility of the end user to scan

diskettes and transferred files they receive. Scanning should be automated when available.

- End users must not disable real-time scanning nor should they use anything beyond the standard product tools to inoculate discovered viruses. If additional support or tools are required, the user should contact their designated Help Desk or Information Security.
- Diskettes destined for customers or suppliers must be scanned before they are released for delivery.
- To allow prevention of macro viruses, users must use application default extensions for documents (i.e., <filename>.doc). In the event that a business unit establishes other standards for application file extensions, these standards must be communicated to the server administrator(s) for all servers where such documents are stored. This ensures files with such non-standard extensions are included in virus scanning cycles.

14.4 Software Oversight

A software oversight team or a central software distribution group should monitor and report virus activity as well as maintain procedures that provide for the effective implementation of practices to ensure swift identification, eradication and recovery. The purpose of the oversight team is to ensure consistent and diligent attention to virus issues within the organization.

14.4.1 Software Oversight Team

- Team Leader: Information Security Program Manager
- Team Members: Information Security Team Members (IS)
Help Desk Personnel and Management
Distributed Computing Resources
Software Distribution Resources
Organizational Unit Representatives

14.4.2 Oversight Team Responsibilities

- Address new virus risks and exposures.
- Defining effective protection and eradication procedures and practices.
- Ensuring awareness and educational programs are in place including information about user responsibilities and procedures for safe computing practices.
- Monitoring, reporting and taking appropriate actions to minimize the effects of viruses on the computing environment.
- Preparing monthly reports on virus incidents, trends, and issues for all team members and the Information Security department.

15 Information Security Incidents

This standard applies to the entire computing environment, including personal computers, networks and applications. Intent of this section is to establish guidelines for the prevention or minimization of information and financial loss resulting from information security related incidents.

An incident is an unexpected, unplanned event, usually involving a security breach that could lead to significant financial loss and/or embarrassment.

15.1. Responsibilities

- Business units that own or are responsible for systems and/or networks are accountable and responsible for coordination of local monitoring, alerting, and response to security related incidents in compliance with Information Security standards. All business units should have system resources connected to available centralized intrusion detection systems, vulnerability assessment and compliance monitoring tools as provided by Information Security.
- A Computer Emergency Response Team (CERT) should be established and responsible for responding and acting on information security incidents. Business unit personnel responsible for maintaining the enterprise environment must comply with Information Security policy and provide adequate, reasonable and timely resources to the CERT, as required when investigating an incident.
- Information Security must promptly analyze potential security incidents to determine validity, impact, and the level of immediate and future risk to the organization. Information Security is responsible and should be empowered to take prudent actions to limit any further damage.

15.2. Standard Incident Response Procedure

When an information security incident is detected, the following steps must be taken:

- Assess the risk of the incident
- Reestablish/implement additional security controls or, with management direction, monitor the exposure with the intent to collect evidence
- Collect and secure evidence
- Identify how the incident occurred
- Deploy additional countermeasures to prevent recurrence
- Determine any consequential or punitive action; consult Human Resources (HR) when employees are involved

15.3. Incident Response Requirements

- When investigating an incident, a business unit must inform all other business units that may potentially be impacted by the incident. Upon completion of response activities, any incident resulting in financial or information loss, compromised system access controls must be documented and reported to Information Security.
- When collecting evidence, certain information must be captured whenever it is suspected that a computer crime or abuse has taken place. The relevant information must be securely stored off-line. The information must be collected immediately and should include copies of all relevant system and data files. These procedures must be followed in order to secure evidence and ensure it is not modified and is therefore admissible in court.
- All security related incidents and/or activities must be documented and reported to the Enterprise CERT even when properly addressed at the business unit level.

15.4. Enterprise Computer Emergency Response Team (CERT)

The overall purpose of the CERT is to ensure consistent and timely response to all security related incidents. The Enterprise CERT acts at the time of an information security incident to minimize and contain damage, gather evidence and resume normal processing. The CERT also provides guidance and/or recommendations to prevent or minimize the reoccurrence of security related incidents. .

15.4.1. Membership and Meetings

- Team Leader: Information Security Manager
- Team Members representing:
 - Information Security
 - Outside Investigative Agencies
 - Physical Security Authorities
 - Human Resources (HR)
 - Legal
 - Impacted System Administrators, DBAs, Network Engineers, etc.
 - Business Unit Representatives
 - Operations Personnel
- Meetings: As needed.

Each unit has a primary and back-up member. Members may need to respond at any time from any location. Therefore, management should consider the nature of the assignment before designating team members. Business unit technical resources should be available as needed.

15.4.2. Response Team Responsibilities

The Emergency Response Team is a comprised of internal experts responsible for responding to corporate information security incidents in order to limit and contain damage, recover information, pursue remedies for losses, and investigate and ensure corrective action. Specific responsibilities include:

- Defining and classifying incidents
- Developing and maintaining procedures for:
 - □ Incident response escalation and communication
 - □ Tracing intrusion attempts
 - □ Collecting and securing evidence
 - □ Mitigating damage from an incident
 - □ Resuming normal processing after an incident
 - □ Reporting requirements
- Following incident response procedures
- Determining the tools and/or technology to be used in incident detection, prevention and evidence collecting
- Determining if the incident will be investigated and the scope of any investigation
- Determining interface and protocol for when and how external entities (law enforcement agencies, outside expertise/consulting, etc.) should be involved
- Protecting the impacted environment
- Conducting postmortem reviews
- Determining resultant actions
- Actively participating with national and international response team organizations, including:
 - □ CERT Coordination Center, Carnegie Mellon University
 - □ CIAC - U.S. Department of Energy's Computer Incident Advisory Capability
 - □ FIRST - Forum of Incident Response and Security Teams, world-wide federation formed by the CERT

15.4.3. Business Unit Responsibilities

Business unit management and personnel with responsibilities pertaining to the administration and maintenance of the computing environment must cooperate and provide adequate, reasonable and timely resources to the CERT as needed to fulfill the team's responsibilities.

16 Information Ownership and Data Access Strategy

Business managers are responsible for their information assets and data. All information assets and data must be associated with an owner. All information related to the organization is considered proprietary and will be protected from unauthorized access or disclosure. Access to proprietary information must be authorized and the information accessed must be applicable to one's job function and role.

16.1. Data Access Strategy

All business units with electronic information assets and/or data must have a documented Data Access Strategy. A Data Access Strategy is a standard format document that identifies:

- Inventory of information owned (file and data descriptions)
- The information security (risk) classification of this information
- User access requirements
- Processing platform, system and application requirements for the information
- Information Security personnel designated for oversight and any available access review schedules

And defines:

- How access privileges are authorized and granted and by whom
- Implemented monitoring services

The purpose of a Data Access Strategy is to:

- Ensure data is adequately secured by minimizing the risks and exposures of excessive and/or inappropriate access capabilities.
- Identify data stewards and information security administrators who are accountable and responsible for understanding, defining and documenting this strategy within their business unit.

16.2. Data Access Strategy Roles and Responsibilities

The data steward is the business manager who makes business decisions concerning specific business processes, products and/or services. The data steward is primarily accountable and responsible for establishing and maintaining security controls for information created and/or maintained as part of the business. The data steward is responsible for the Data Access Strategy. It is also the data steward's responsibility to assign the role of information security liaison for the specific business function.

The data steward or designee responsibilities include:

- Determining the value and criticality of the data through the use of an authorized risk assessment method. Such an assessment will allow for an appropriate classification of the data.
- Assessing exposure for unauthorized access to data.
- Creating and maintaining the Data Access Strategy.
- Determining data needing access controls and job functions allowed access.
- Approving access controls and procedures established by the security liaison.
- Implementing local procedures to ensure changes within the unit, which affect established access controls (i.e. new applications, application enhancements, etc.) are identified and incorporated into the Data Access Strategy.
- Ensuring the Data Access Strategy complies with all organizational information security policies, standards and procedures.

The security is responsible for implementing access controls as defined by the data steward and the Data Access Strategy. This includes:

- Being knowledgeable of a business unit's data processing resources.
- Reviewing requests for data access and approving or denying them.
- Follow established procedures when submitting access control requests to a Security Administrator.
- Coordinating information security maintenance which includes:
 - □ Logon ID maintenance (setups, changes, transfers, terminations, etc.).
 - □ Maintenance to rules determining access capabilities to data.
- Implementing procedures to ensure that the proper access controls are in place, including an audit trail showing all actions taken.
- Reviewing reports of access logs and failed access attempts with necessary follow-up on a timely basis.
- Other monitoring security activities including reviewing logon ID lists and access rules/paths to data for validity and appropriateness with follow-up to eliminate any found exposures.
- Investigating suspected/actual incidents.
- Recommending changes to the Data Access Strategy.
- Communicating information security requirements to custodians and users.

Both the data steward and the security liaison are responsible for:

- Monitoring compliance with information security policy, standards and procedures.
- Promoting information security awareness.
- Contacting Information Security when exceptions/incidents occur.

Information Security should designate a security administrator for Information Processing functions. Business unit management can be allowed to assign security administrators in the

case that Information Security has approved decentralized security administration. The security administrator is responsible for implementing access controls for systems resources. This includes:

- Processing/implementing security requests approved and forwarded by a security liaison.
- Managing the access control system. Such a system must allow authorized users minimal access to data, prevent and log unauthorized access attempts, and provide for user identification and passwords. Passwords must be compliant with current organizational standards of configuration for Information Security.
- Reviewing and distributing access control reports.
- Investigating suspected/actual unauthorized access attempts, documenting findings and reporting to management. If security administration is decentralized, then Information Security must be notified as well.
- Ensure that password changes are made according to current organizational standards.

16.3. Data Access Strategy Requirements

- Business unit management is accountable and responsible for their electronic data, including validity, integrity and security. A Data Access Strategy will document procedures and controls in place to ensure that these responsibilities are upheld.
- The Data Access Strategy must define who should have access to data and application functions, what kind of access and under what circumstances that access may be granted. Grouping access privileges based on identified job functions/responsibilities is most appropriate.
- The Data Access Strategy must also define required information security controls and procedures of audit trails, system monitoring and review of sensitive transaction/activity logs.
- The Data Access Strategy Guide defines in detail all the information and elements required in a Data Access Strategy.
- The Data Access Strategy must be reviewed annually at a minimum and updated whenever changes are required.
- Suspected/actual attempts to breach access control must be reported immediately to management and to Information Security.