INTERNAL USE ONLY

# Electronic Information Security Standards (EISS)

***Version 1 Edit 3***
***5 January 2007***

INTERNAL USE ONLY

## Table of Contents

# EXECUTIVE OVERVIEW

Computer systems store our intellectual property and are prominent targets of fraud and other forms of computer misuse and abuse. The terms fraud, misuse and abuse exhibit themselves within a broad range of activities. These range from unintentional errors to acts of malicious damage, stealing information or intellectual property, violating privacy, and committing financial fraud. Computers and networks have changed commerce and the manner in which SDLC electronically conducts business as well as the nature of computer fraud. Much of this fraud and abuse dictate the need for computer security standards and can be controlled by improved information security practices.

Council, the Enterprise Messaging Council, and the Firewall Task Force. The basic framework for establishing these standards is not stand-alone, but has been based from, and supplements existing SDLC Policies and standards including but not limited to:

Standards of Internal Control (SIC's)
Standard Operating Procedures (SOP)
World-Wide Corporate Financial Policies
SDLC Corporate Security Policy and Procedure Manual
SDLC Data Network Architecture Standards

**Purpose**

The purpose of these standards is to define and establish a consistent set of information security controls required to protect SDLC's information assets and intellectual property. Sector/Group standards and policies may define more stringent controls where business requirements dictate them.

These Electronic Information Security Standards have been developed to provide reasonable controls for protecting SDLC from a wide variety of threats which could cause damage by allowing security to be violated. They have been built around a framework where real-life threats and vulnerabilities have been identified, and controls have been selected and established which allow the threats to be reasonably safeguarded and contained. Safeguards and reasonable controls recognize that the cost of the controls should not exceed the benefit to be derived.

**Scope**

These standards apply to security, integrity, availability and confidentiality of information obtained, created, or maintained by any SDLC or Non-SDLC staff accessing a SDLC information asset. These standards also apply to all service providers and joint ventures where applicable.

**Summary of Revisions**

1. Originated
2. Reviewed for content, consistency & clarity
3. Revised for SDLC

# 1.0 INFORMATION MANAGEMENT STANDARDS

**Purpose**

SDLC is an information-intensive company. Its employees and contractors need accurate, dependable, and current information to successfully compete in the marketplace.

The purpose of this section is to define the minimum standards that apply to managing SDLC's information assets, and the information assets of other companies or entities held in SDLC's custody.

**Scope**

These standards apply to all SDLC employees, contractors, agents, EDI trading partners, SDLC's customers, or other organizations that access SDLC assets. These standards pertain to all information contained on electronic media. Sectors or groups may wish to extend these standards through publication of local standards; especially if there are more stringent security requirements levied by clients or government agencies. Wherever government requirements are in conflict with these standards, the government standards will prevail.

The scope of these standards covers all internally used computer systems, no matter the type of platform, as well as any intelligent device that is part of, or manages a network. Included are all mainframe computers, minicomputers, computer workstations and personal computers (PDA's). These standards are applicable to local area networks, premise distribution networks, campus or metropolitan networks and wide area networks.

**Background**

SDLC uses a wide variety of electronic information processing, storage, and communication systems around the world. Computer storage, voice mail, fax, and video tape are several examples of the many different electronic media used to store business information. World-wide partners of SDLC, customers, suppliers, and governmental employees (local, US and foreign) share SDLC's electronic systems to process information.

Since information is an important resource, it must be protected to a level that corresponds to its value to SDLC. To stay valuable, data must have the following characteristics: availability, integrity, and confidentiality. Security programs, good system development practices, and established supervision and training procedures are all necessary to ensure information quality.

The publication of these standards is not intended to modify or in any way nullify any local legislation on the subject of information security in any of the SDLC operating countries. For example, in Europe there exists a variety of national laws, protecting the rights of citizens against unlawful, inaccurate, unfair or unauthorized collection, processing, transmission or storage of personal information relating to individuals. Departmental management must, with the guidance of local Human Relations and Law departments, in each country, ensure compliance with the aforementioned legislation.

Section 1.0 entitled "Information Management Standards" discusses the general management of information in the following subsections. These basics apply to all other standards contained throughout this manual.



## 1.1 Legal Ownership of Information

This sections states the security standards relating to the ownership, access, and use of SDLC information.

**1.1.1 Ownership**

SDLC considers all data on SDLC computers or networks as existing for the purpose of conducting SDLC business.

a) All SDLC data is in the custody of those that handle it. As company assets, these resources are subject to the same regulations and controls as any other asset of the company.

#### 1.1.2 Access

SDLC provides information to employees, contractors, agents and other business partners in order for them to perform their jobs.

a) Access to information is provided in an environment that is sufficiently controlled to provide the following:

- **Integrity** (safeguarding the accuracy and completeness of information and computer resources),
- **Availability** (ensuring that information and vital services are available to users when required), and
- **Confidentiality** (protecting sensitive information from unauthorized disclosure or intelligible interception), so as to minimize the risk of disclosure, misuse, or loss due to accidental or deliberate means.

#### 1.1.3 Appropriate Usage

No person may use SDLC electronic devices or resources for private or personal purposes without management approval. Willful misuse is grounds for disciplinary action.

## 1.2 Ownership and Custodians Roles

The concept of owners and custodians for computer systems, files, and programs is defined in Standards of Internal Control.

SDLC managers at the enterprise, corporate, sector, group, division, or departmental level must maintain formal documentation on assigning an owner for each information asset. Information assets could include databases and data files, application systems, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, application system or collection of data. Ultimate responsibility for information used by the application system is held by the corresponding system owner. Owners must be aware of their responsibility.

#### 1.2.1 Custodian's Role and Authority

Custodians of information assets are personnel who support and maintain information systems, computers and telecommunications equipment. They provide physical asset control suitable to the classification of data under their custody to ensure the confidentiality, integrity and availability of information. Custodians are usually personnel that support the development and maintenance of application systems, or collections of data, and/or computer/network equipment.

a) Custodians of information must provide physical and procedural safeguards as appropriate to the classification of information in their custody, to ensure the integrity and confidentiality of information assets as identified by information asset owners.

b) Each information system is an asset, therefore an owner must be clearly defined and documented. Owners are assigned the responsibility for the maintenance of appropriate security measures which may be delegated. Where appropriate an alternate contact must be identified. Custodians must keep a list of system owners.

c) Custodians must inform information asset owners of their responsibilities associated with the ownership and security of their data.

d) Custodians must not reclassify information without the permission of the owner.

#### 1.2.2 Owner's Role and Authority

The owner of any information asset is the person(s) who owns the data. They typically have overall responsibility for the data itself, it's data classification, and control of whom has access to the data. Ownership includes the right to create, classify, retrieve, modify, delete, or archive owned information. The owner authorizes access privileges to others on a need-to-know basis. Owners and custodians are jointly responsible for ensuring the availability of information assets.

a) All information assets must be accounted for and have a defined owner. An owner is an individual or organization responsible for the specified information asset(s) and the application of appropriate security measures as they pertain to these assets.

b) Owners and their managers are responsible for performing a risk analysis to determine, identify, and document the security classifications associated with the information assets they own in accordance with POPI classifications (Section 1.3.1). This classification must be reviewed at a minimum annually.

c) Owners are responsible to ensure that the appropriate business controls are applied, and that the conditions surrounding the custody or use of their information is in accordance with the requirements of SIC and this document.

d) Owners are responsible for assigning the role of custodian to their data, or fulfilling that requirement themselves.

e) Owners must fully understand any custodian conditions surrounding the custody or use of their information and ensure it is in accordance with the requirements of SIC and this document.

f) Owners are responsible for granting access privileges to those needing access to their data on a need-to-know basis.

g) Owners must review access privileges to their data annually at a minimum. The review process must be documented and renewal information retained for a minimum period of one year.

## 1.3 Information Classification

Information security is required in all SDLC computer system environments. An effective security program starts by taking inventory and evaluating the availability, confidentiality and integrity of the information in the system.

The term "sensitive information" refers to information that can result in loss to the corporation if it is accessed by or disclosed to unauthorized parties, or if it is fraudulently modified or updated. Sensitive information may also refer to data that is sensitive to individuals, for example, relating to their health or personal information. Access controls, change controls, integrity controls, and audit trails, protect sensitive information.

Information sensitivity may be time dependent. Often, information is classified at a high level until a new product is announced information is released to the public or a court case is settled. Therefore classification schemes must be responsive to time, and "downgrading" process as defined in SOP must be performed.

All employees, as agents of SDLC, share in the responsibility for the protection of SDLC information, particularly when sensitive in nature. Examples of sensitive information include:

- Information proprietary to SDLC as defined in the SDLC Protection of Proprietary Information Policy (Section 1.3.1);
- Information which, if manipulated, can cause financial loss (e.g. fraud, embezzlement).
- Information proprietary to others that SDLC holds as a trusted agent.

The term "critical information" refers to information that can cause a loss or serious disruption in the corporation's ability to function if the availability of the information is denied or impaired. The criticality of information describes the data in terms of its effect on the company to perform its normal operations, management to make decisions, and competitive position.

Classification of information is clearly defined in Section 1.3.1.

**Proprietary Information**

According to POPI (Section 1.3.1), "proprietary information" refers to all information useful to SDLC business which SDLC has legal rights to, is not common knowledge outside the company, or improves SDLC's competitive position.

Proprietary information includes, but is not limited to, trade secrets, leading edge technical information, and knowledge of any business or financial opportunity. Information is also considered proprietary if its disclosure causes the loss of a competitive advantage or the invasion of privacy to SDLC or any of its employees.

#### 1.3.1 Protection Of Proprietary Information (POPI) Information Classification Table

The following table describes the classification responsibility and instructions for use and handling SDLC POPI data classifications. A subsection that further clarifies security requirements in each of the POPI information sensitivity classifications immediately follows it.

| POPI Classification of Information | Type of Information | Classification Responsibility | Instructions for Use |
|---|---|---|---|
| General Business Information | Information that is owned by our business that is not otherwise classified. (e.g. a copyright brochure.) | Assigned by the person creating or gathering the information. | ***WHO***: All those with a legitimate business need for the information.<br>***MARKING***: No special requirements.<br>***HANDLING***: No special precautions.<br>***DISTRIBUTION***: Any appropriate method.<br>***DESTRUCTION***: No specific requirements. |
| SDLC Internal Use Only | Information that could benefit our competitions at our expense. (e.g. a phonebook or internal memo) | At a minimum, must be assigned by the person who created or collected the information | ***WHO***: Anyone with a need to know<br>***MARKING***: "SDLC Internal Use Only" on the first page<br>***HANDLING***: Keep in control<br>***DISTRIBUTION***: Approved E-Mail or electronic file transfer systems.<br>***DESTRUCTION***: Ensure non-SDLC staff cannot acquire material. |
| SDLC Confidential Proprietary | Information that has a significant value to the company. (e.g. financial statements) | At a minimum, must be set by the department manager of the organization creating and managing the information. | ***WHO***: Need to Know, requires a confidentiality agreement.<br>***MARKING***: "SDLC Confidential Property" on every page<br>***HANDLING***: Keep in possession or locked<br>***DISTRIBUTION***: Approved E-Mail or electronic file transfer systems with access control.<br>***DESTRUCTION***: Shred or place in secure document receptacles. |
| SDLC Registered Secret Proprietary | Information that is most sensitive in nature. (e.g. trade secrets, chip design) | At a minimum, must be set by a Director-level or higher executive of the organization creating and managing the information. | ***WHO***: Need to Know, requires a confidentiality agreement; access determined by a vice president.<br>***MARKING***: "SDLC Registered Secret Proprietary" on every page<br>***HANDLING***: Keep in possession or locked<br>***DISTRIBUTION***: Secure electronic systems with access control and encryption<br>***DESTRUCTION***: Return to originator |

#### 1.3.2 SDLC Registered Secret Proprietary

This classification describes information that is of the most sensitive nature. Examples include certain formulas or designs, future market plans, strategic acquisitions or divestitures, user plans and top management strategies.

a) Dissemination must be limited to the smallest possible group of selected individuals
b) A Vice President-level or higher executive of the organization creating and managing the information must minimally set this classification.
c) Must be marked "SDLC Registered Secret Proprietary".
d) Must be kept in possession or under lock and key.
e) Must be returned to originator for destruction

#### 1.3.3 SDLC Confidential Proprietary

SDLC Confidential Proprietary includes information that has significant value to the company. Examples include personnel information, tactical plans, pricing/marketing practices and product designs.

a) SDLC Confidential Proprietary information must be limited to persons with a need to know.
b) The department manager of the organization creating and managing the information must minimally set this classification.
c) Must be marked "SDLC Confidential Proprietary" on every page.
d) Must be held in possession or under lock and key.
e) Must be "dot" shredded or placed in secure document disposal receptacles.

#### 1.3.4 SDLC Internal Use

SDLC Internal Use Only is any information, which, if communicated outside SDLC, could benefit others at SDLC's expense. Examples include organization charts and internal memos on sensitive subjects.

a) Information classified as SDLC Internal Use Only must be limited to SDLC Staff and authorized non-SDLC Staff.
b) The person who created or collected the information with their manager's approval must minimally set this classification.
c) Must be marked "SDLC Internal Use Only" on the first page minimum.
d) Must be disposed of so that non-SDLC staff can't acquire it.

#### 1.3.5 SDLC General Business Information

Any information "owned" by SDLC and used for business purposes that does not fall into the other information sensitivity classification is considered SDLC General Business Information. This information may be widely available, but is still the property of SDLC.

a) This classification must be assigned by the person creating or gathering the information, with their manager's agreement.

#### 1.3.6 Assigning Classifications

This section defines the security process for assigning classifications, the security requirements for classifying data output, and the process for handling requested access.

Process for Assigning Classifications:

a) The organization and management that "owns" the information (usually the creator) must determine its sensitivity and criticality classification.
b) Information sensitivity to disclosure or manipulation must be assigned according to POPI (Section 1.3.1)
c) Proprietary Information and information that is highly sensitive to outages must be identified in disaster recovery plans as described in this document.
d) Information Classifications must be reviewed at a minimum annually by the business unit that owns the information to ensure that the classification is still correct.

Classifications of Data Output

e) Any output, including report, data, and software, which contains the same information content as the input used to create it must be assigned the same sensitivity classification or higher as the input.
f) Any output that is formed by the merger of multiple inputs must be classified in accordance with the highest level of sensitivity classification or higher represented by the input.
g) Any output that is substantially different than the input information used to create it, must be classified independently from the input.

Access

h) System or application owners must authorize access to their data or applications in accordance with of the SIC's.
i) Access authorization must be reviewed on a yearly basis in accordance with SIC.
j) System, application or data owners must identify resources to administer access.

#### 1.3.7 Non-SDLC Proprietary Classification

There are instances where SDLC is in possession of information that actually belongs to other companies (e.g. suppliers or customers). Information that does not belong to SDLC may contain markings of its proprietary status that do not follow the POPI classifications. However, such information must be correlated to the appropriate POPI classification

a) It is the responsibility of the SDLC staff member who receives the information to ask a non-SDLC information owner to define the meaning of any non-SDLC information classification label.
b) The non-SDLC proprietary classification, along with the SDLC equivalent classification must be marked on information that is not owned by SDLC and is considered proprietary based on the original owner's classification scheme.
c) All use of non-SDLC proprietary information while in the possession of SDLC must be treated with the same care as defined by the closest corresponding SDLC POPI classification. For example, if a vendor supplies information to SDLC labeled as sensitive, it is the responsibility of the SDLC representative to have the vendor define the classification label to determine if the information is proprietary and equivalent to SDLC Confidential Proprietary or SDLC Registered Secret Proprietary.
d) If non-SDLC information has been given to SDLC and it has not been altered in any way it can be returned to the original owner without the need for a signed non-disclosure.

## 1.4 Information Privacy Standards

There are no global laws or standards in existence today that define personal, private, or sensitive data, let alone how such data can be handled or processed while protecting the rights of individuals against unlawful, inaccurate, unfair or unauthorized collection, processing, transmission or storage.

a) Regional and resident local in Country Management, with guidance and advice from local Corporate Law departments are responsible for ensuring compliance with applicable law legislation.
b) Regional and resident local in Country Management must ensure that SDLC ethics principles are enforced, and that the individual's personal and business privacy is not willfully violated.
c) Management, Human Resources personnel and system administrators must be especially diligent when handling personal and private data.
d) Any information system handling personal and private data must comply with applicable data protection laws, which may also cover manual records.
e) Any disclosure of personal data, for example in the course of problem resolution, must be kept to an absolute minimum.
f) A person must be assigned to be responsible for local or country data protection issues which covers any SDLC site, to ensure compliance with these privacy standards, and national and international legal requirements, including registration with data protection authorities. The person will make recommendations on the amendment of existing systems and the introduction of new ones, and act as liaison with their local corporate law department who would be able to resolve any major SDLC policy or legal issues.

# 2.0 GENERAL SYSTEM INTEGRITYAND SECURITY ACCESS CONTROLS

**Purpose**

To state the security standards which support the SDLC Information Security Policy for protection of computer-based data (also known as the Protection of Proprietary Information Policy, POPI, or Section 1.3.1).

**Scope**

These standards apply to all SDLC computer systems unless specifically addressed elsewhere in this document.

The information contained in this section is intended to supplement the standards already specified in the SDLC Standards of Internal Control (also know as SIC.)

All of the electronic facilities used at or connected to SDLC must meet the general requirements established in this chapter.

In general, secure information systems will control access to information through use of specific security features so that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, modify, create, or delete information.

Section 2.0, entitled General System Integrity and Security Access Controls, includes the following subsections:

| | |
|---|---|
| Subsection 2.1 | Security Access Controls |
| Subsection 2.2 | Specific Access Controls |
| Subsection 2.3 | Data and Resource Controls |
| Subsection 2.4 | Systems and Security Administration |
| Subsection 2.5 | Audit Trails and Verification |
| Subsection 2.6 | Security Vulnerabilities |

## 2.1 Security Access Controls

As computer systems continue to grow in ability for supporting business capabilities and integrate with other networks, the challenge of keeping them secure becomes increasing more important and difficult. The ability to communicate across networks, and share information creates a potential for unauthorized access and financial loss if proper security access control is not considered and implemented.

Many security access control products exist as add-ons or enhancements to existing systems. Operating system vendors often add security services to newer releases of their software. Third party vendors often offer security add-ons to existing software or hardware products. Many computer systems have one or more administrative system utility programs that are sometimes capable of overriding system and application controls.

The role of security access control is to provide a means of identifying a person desiring access to a computer and information, to validate that person's identity, and to validate that the person is authorized to perform the requested operation. This section identifies the security access controls that are required within SDLC, and describes the security requirements for implementing additional security software products.

a) Security controls must be installed, available and maintained on every computer or node to prevent unauthorized users from gaining entry to the system, to prevent unauthorized access to data contained on, or accessible through the system, and to ensure the availability of data and computing resources. (SIC)
b) Security hardware/software must provide a means to authenticate a user's claimed identity.
c) Security controls must protect user authentication data so that any unauthorized user cannot access them.
d) All SDLC information assets must be protected by security hardware and/or software products which have been approved by the Information Security Council in conjunction with Sector, Group and Corporate Information Security Organizations.
e) Programs or routines which are capable of bypassing or modifying the security system, operating system integrity features, or any application security controls or data are expressly prohibited unless approved and administered by authorized security personnel. If approved it must be verified to ensure that the process is only doing what it is authorized to do. The implementation, use & results of such program or routine must be documented & classified confidential.
f) Software which is capable of running in system protected areas, under privileged ID's, or that is capable of granting special privileges must only be setup, tested, and executed by a limited number of trained, trusted, authorized personnel (generally system or security administrators). Procedures must be documented and in place that describe software

implementation, use, and ensure that the operation of such software does not compromise security.

g) Security software and privileged administrative utilities must be approved and documented, and usage logged and limited to authorized and documented security changes.
h) Administrative password protection must be implemented for all system and security utilities. Default administrative account passwords for such software must be changed during product installation
i) Tampering with or removing any SDLC security software/hardware controls is a disciplinary offense per SOP.

## 2.2 Specific Access Controls

The subject of system access controls includes a number of topics, each relating to controls for gaining access to a computer-based SDLC system. The following topics are covered in this section

- Computer Accounts
- Passwords and Account Verification
- Other System Access Validations

#### 2.2.1 Computer Accounts

A computer account is the means of access to SDLC data and computing resources. There are three types of computer accounts:

- User Accounts
- Special Function/Application Accounts
- Non-SDLC Accounts

The following standards apply for all types of computer accounts.

a) The login ID assigned must be unique within its own system domain and all other domains in which it will be used. There must be some way to easily identify the ID with the individual using that ID. (** Note: In certain circumstances, administrative accounts, such as root, supervisor, administrator, or application account login id's such as ClearCase, arc serve, LanProtect are not able to able to remain unique due to the nature of the purpose of these accounts.)
b) A process must be in place to identify all accounts associated with a given user.
c) Explicit management approval must exist for each computer account. This documentation must be retained as long as the account remains on the system.
d) Every computer account must have a defined owner who is responsible for all usage of that account.
e) No anonymous, group or guest accounts are permitted on any protected SDLC system.

#### 2.2.2 User Accounts

User accounts are accounts assigned to a particular individual who is responsible for all transactions that take place under that account. This section defines specific standards for the assignment of SDLC User Accounts.

a) All SDLC Staff must be assigned a user account with an individual login ID to access any SDLC system.
b) The login ID must be associated with a single individual, and not be shared with another person.
c) In situations where there is a business reason to allow an individual other than the User account owner to access their account, controls must be in place and documented which require management approval and ensure that the password is immediately changed when the account owner returns. Examples include situations where an individual my be placed on immediate medical leave, access may be required due to extended travel, or rotating administrative positions that are filled by different temporary personnel. A login ID may be retained by the person upon transfer to new organizations within a group or sector with agreement between the gaining and losing data security administrator.
d) Access to any system or node must require users to identify themselves or to have previously identified themselves via a computer account before performing any system actions or functions.
e) A login ID may be retained by the person upon transfer to new organizations within a group or sector with agreement between the gaining and losing data security administrator.
f) A login ID is security sensitive. It cannot be treated as SDLC General Business Information and may not be printed on stationary or business cards. 'Friendly' email aliases are General Business Information and may be printed provided they are not associated with the actual login ID.

#### 2.2.3 Special Function Accounts

Special function accounts are accounts that are functional in nature but where a specific individual is responsible for activities performed under that account. Examples of these types of accounts include administrative accounts, accounts that are activated by another computer or are associated with system services such as "daemons" or "detached processes". This section defines the additional requirements for these types of accounts.

a) Special function accounts may not be used as a replacement for user accounts.
b) The need for the use of special function accounts must be documented and approved by management. This documentation must include at a minimum, the following information:

- The ID that has been established for the account
- The primary owner of the account - generally the requester
- The specific business requirement for use of this account
- A list of individuals who have access to usage of this account, or knowledge of the account ID and Password
- The documented process that describes how this account will be maintained. This documentation must include how password changes will be controlled, how usage will be reviewed regularly to ensure that individuals who have access to this account still need it, and procedures for changing the account password when individuals who use this account change jobs or separate from SDLC.

c) Access to special function accounts must require users to identify themselves or to have previously identified themselves via a computer account before performing any system actions or functions under that account OR all usage activity of special function accounts must be logged to identify the individual using the account. These logs must be retained for a minimum period of a year.
d) Special function accounts must be reviewed at a minimum annually to ensure that the account is still needed, and that those that have access to this account still require it to perform their jobs.

#### 2.2.5 Non-SDLC Accounts

To obtain an account for non-SDLC Staff, including contractors, all required agreements with the approvals as described in WWCFP A-6 must be completed (SIC). The requirements for A-6 approval of a contractor include:

a) A legal contract or agreement signed by an authorized SDLC staff member must exist with the contractor and/or the company they represent.
b) A written assertion of need for the contractor to access specific SDLC systems/networks included in the contract or in signed letters/memos between the contractor and the SDLC manager with authority to enforce contract provisions.
c) A non-disclosure agreement signed by all contract employees with ownership and responsibility for a particular user account
d) All non-SDLC staff accounts are subject to all of the SDLC security policies, standards and guidelines.

#### 2.2.6 Account Administration

Lack of adequate account administration subjects systems to breaches of security. This section defines the standards for administering accounts.

a) Computer accounts must be suspended immediately when an individual is removed from active employment status or is on short or long term disability unless management and Human Resources have approved it.
b) Accounts must be suspended immediately upon the termination or separation of an individual from SDLC.
c) A documented process must be in place to periodically search for, review, and suspend inactive (non-login) computer and user accounts. This must be done at a minimum quarterly.
d) Accounts that are accessed at intervals greater than three months must be suspended until needed again, unless there is an approved exclusion list or reinstatement is anticipated.
e) Suspended accounts must be deleted after six months of continual suspension, unless there is an approved exclusion list or reinstatement is anticipated. Active or needed files that otherwise would be deleted must be reassigned.

#### 2.2.7 Password Security and Account Verification

Passwords are a primary means of system access security. Without good password security, all other means of protecting computer data may become ineffective.

Password security depends upon good password selection. It has been demonstrated that unauthorized system entry often depends on repeated trial and error attempts with commonly used passwords.

Using other user authentication methods in addition to passwords, such as smartcards or biometric scanners, further strengthens the user validation process. This section defines security requirements for passwords and personal identification numbers (PINs) which are used as authentication mechanisms.

a) Passwords must not consist of commonly recognizable names or words, readily guessable sequence of letters or numbers, or data that can be easily associated with the user, such as birthdays, names of self, spouse, children, etc.
b) Password length must be a minimum of six characters. Where feasible, 10-12 characters strengthen password security
c) Computer account passwords must be changed at a minimum, every ninety days.

d) Special function account passwords that are used to connect one computer to another minimally require annual password review and change.
e) System administrator, security administrator, privileged, and special function accounts that perform privileged functions must change their password at least every thirty days.
f) System and security administrative passwords must be changed whenever there is a change in administrative responsibility. This includes all accounts that may have been known before the change in responsibility or separation occurred.
g) The same password must not be reused by a given account for a period of one year.
h) A login session must be terminated after a maximum of three consecutive invalid login attempts.
i) General computer accounts must be suspended after seven invalid login attempts occur since the last successful login. Standard administrative accounts, such as root, administrator, or supervisor must never be suspended as their suspension could create a denial of service. Alternatively the system must insert a time delay that increases with each attempt so as to make brute force guessing attacks infeasible.
j) The length and composition of passwords and authentication tokens must be automatically enforced by the security system.
k) The system must enforce password changes automatically (SIC).
l) The system must not display or legibly print a password.
m) Automated logon procedures may only be used where suitable security measures have been implemented which prevent unauthorized use of the computer account and/or disclosure of the password.

#### 2.2.8 Password Confidentiality

Everyone must understand the need for maintaining confidentiality of passwords. The world's best password is ineffective if it has been compromised. This section defines the specific security standards relating to such confidentiality.

a) A password must be treated as SDLC Confidential Proprietary information at a minimum, and as SDLC Registered Secret Proprietary if protecting SDLC Registered Secret Proprietary information.
b) Passwords must not be posted or exposed to the view of others.
c) Passwords must be changed immediately if it becomes, or is suspected of having been compromised. Plain text, non-encrypted passwords must not be written or stored in or on any computer generated or accessible media, such as disk, tape, or printed material -unless the paper or media is stored in a place accessible only by the owner of the account(s) protected by the password and/or under lock and key. The communication of an initial or changed password is the only exception to this rule.
d) Plain text, non-encrypted passwords must not be retained in computer storage or memory for longer than necessary to do the required processing.
e) Passwords must be one-way encrypted, per the standards in Section 3.0.

#### 2.2.9 Password Administration

The need to protect passwords is a concern to both computer account owners as well as system and security administrators. Password mechanisms work only if passwords are kept secret at all stages. Administrators must establish a viable way to protect passwords. This section defines the security standards for password administration.

a) A secure method must be documented and used when distributing passwords. This must include some verification of the identity of the person to whom the password is distributed to, such as the presentation of their valid badge, etc.
b) Accounts must be suspended if the user does not replace a pre-established password within ten business days. Accounts where the user access level is classified confidential or above must replace a pre-established password immediately upon activation of that account.
c) Administrators must have a documented procedure for responding to password change requests and ensuring the identity of the requester when passwords are changed and redistributed.
d) Administrators must ensure that password files are protected from unauthorized access.
e) A documented process must exist and be followed describing how administrative or privileged account passwords are changed, logged, distributed, and stored in a secure location so that in the event an administrator is unavailable in an emergency situation, management can obtain this password.
f) For those platforms and types of hosts where the native operating system is not capable of enforcing password provision standards, but for which a third party vendor has developed an "add on" security system or utility to accomplish this, the administrator of the system must install and use it if it has been approved for use within SDLC.

#### 2.2.1O Other System Access Validations

Basic system access controls check who can access the computer system by confirming the identity of the user based on something a user "knows" or "has". Access controls can also consider under what conditions the user may access the system. Sample conditions include checking the physical source of entry, the time period at entry, the type of computer services requested (such as the class a job must run in), and the department charged for computer services.

a) Measures must be taken to prevent unauthorized use of terminals and personal computers when unattended for any period of time. (e.g. key locks, screen locking, encryption, physical removal, or physical security of the location).
b) The computer user must not leave information classified as SDLC Internal Use Only or higher on the monitor when the monitor is unattended or can be viewed by unauthorized people. Screen locking software must be used and set for no more than ten minutes of inactivity. (Section 4)
c) Where possible procedures must be in place to review patterns and trends of unsuccessful logon attempts for computers containing sensitive or critical data.
d) For those environments, such as production batch, where passwords can not be maintained, additional protective measures must be implemented, such as restricting the account to a single location, job, node and/or terminal.
e) Any process classified as production must be protected so that users or non-production processes may not modify, submit, or affect the production process without proper authorization.
f) Any system, which is part of the SDLC electronic information network, must reside on computer nodes that transmit over connections that conform to Corporate and Sector security standards.
g) Marking must exist at the computer system level to advise users of the highest data security level. When this is not feasible, information sensitivity must be indicated at the directory level if the data stored is SDLC Internal Use or higher.

## 2.3 Data and Resource Controls

SDLC's information assets include data and software. All data and resources are assigned an "owner" responsible for the integrity of that data/resource. Data custodians and data/resource owners are jointly responsible for computer data and resources by providing computer controls to assist owners. This section defines the security standards as they relate to data and resource control.

a) The operating and/or security system must define user authority and enforce access control to data within the system (SIC).
b) The operating and or/security system must be capable of limiting access to objects such as data files, databases, printers, programs or services, on either an individual or group basis.
c) For networked or shared systems user access must be limited to only the data that the data owners have authorized.
d) Access controls for any data and/or resources must be determined as part of the systems analysis and design process for any information system. Proper controls must be defined before the data/resource is created and used by the system. Examples include shared data areas, shared applications, etc.

## 2.4 Systems and Security Administration

Security or systems administrators are the personnel who administer and manage access, data controls and key management systems under a defined set of authorization rules and procedures. They may well hold the title and responsibilities of LAN administrator, System administrator, or Security administrator. In many cases the segregation of duties and limitation of functions is not possible due to the particular technological implementation. When technology permits, the following standards must be enforced. Otherwise, compensating controls are required.

a) Each SDLC business unit or owner of a computer system is responsible for its own security administrator functions (SIC). This does not preclude the use of contractors or outsourcing for the system or security administration function. However, a SDLC manager must supervise all personnel responsible for system security administration of a SDLC network or system.
b) The functions performed in the security administrator role must be specifically identified and authorized (SIC).
c) An audit trail must be maintained for system and security administration functions and actions.
d) System audit functions must be segregated from system and security administration so that the ability to view audit logs of privileged access is segregated from those generating the privileged actions.
e) A process must exist to periodically review system and security administration functions by whoever is responsible for the audit function.
f) The security administrator must perform privileged or security functions from an account that is separate from his/her personal account, and the privileged account must be associated with the user and have a unique login ID/ password.
g) Privileged accounts may not be used outside of their scope of responsibility.
h) Security administrators must work closely with data owners to explain security standards and procedures.
i) Security administrators must save all security authorization requests for at least one year. This correspondence serves as an element in the auditing of security administration activity.
j) A risk analysis must be performed, documented, and approved by management before any system administrative or security administrative functions are outsourced. Management on an annual basis must review this risk analysis.

## 2.5 Audit Trails and Verification

Audit trails/logs can be considered a safety net for access control to SDLC computer systems. If for any reason access control fails to block misuse, audit logs detect it. If an authorized person misuses their rights, audits can detect that. Audit logs also help to assess damage in the event a system has been compromised, in addition to serving as a quality assurance tool in helping reveal

how well security mechanisms are working.

Typically audit data is used to analyze or detect misuse. Auditing can also be preventative, allowing you to take preventative action when used to assist in detecting an accumulation of events that are leading to an act of misuse. Since audit trails are potential evidence for legal or administrative actions, both secrecy and integrity of audit data must be maintained without compromise. There must be standards for retaining logs, discarding logs, and integrity that ensures logging survives any system crashes. This section defines the standards for logging, reviewing, and handling security events.

#### 2.5.1 Audit Data

a) Audit trail records must be captured and contain information needed to determine sensitive events, perform trend and pattern analysis, and analyze out-of-tolerance conditions that would indicate possible fraudulent use of the system (e.g. repeated unsuccessful logons, access attempts over a series of days). These records at a minimum must include the following:

- Date and time of the event
- UserID or computer account
- Type of event and the success or failure of it
- Source of the event (e.g. terminal port, node, etc.)
- Use of authentication keys, where applicable

b) A process must exist and be documented for monitoring and reporting all significant security events. The system/data owner must define the "significant security events" to audit in relation to specific application or data files. This review must be documented and include at a minimum the following:

c) The frequency in which the defined security events are reviewed. The frequency must be based on the data's criticality to the business. How and to whom security events relating to their data must be reported.

d) Defined significant security events must be logged and include:

- Multiple failed logons
- Access at unusual times or from unusual places
- Sudden unexpected increases in volume
- Unusual and/or saturated attempts to system resources
- Significant computer system events (e.g. configuration updates, system crashes)
- Security Profile Changes

e) The system must provide the ability to selectively audit the actions of individual users or objects.
f) Audit logs must be established to audit both privileged access and standard access.

#### 2.5.2 Audit Log Classification Retention and Review

a) The system/data owner is responsible for documenting and specifying the data classification of the logged data, its retention period, establishing the frequency of review required, and for the actual review of the log reports.
b) Audit data must be protected against destruction or change. Audit trail records written for the purpose of logging data and/or resource access must be classified in one of two ways:

- Requiring regular review due to the sensitive or critical nature of the data
- Written for historical purposes only to be archived but not reported on or reviewed until needed.

c) Audit logs must be reviewed with a frequency that allows the detection of unauthorized entry before a significant loss has occurred.
d) Access control violations of sensitive or critical data must be reviewed regularly in order to detect patterns of attempted unauthorized use.

## 2.6 Security Vulnerabilities

Weaknesses are identified which could allow the security of a system to be violated or compromised. This is known as vulnerability. A threat is an event that exploits a vulnerability that could cause harm by violating security. This section addresses the security requirements for responding to known vulnerabilities.

a) All security software, which includes security access software, anti-virus software, intrusion detection software, system scanning software, etc. must be maintained at a level not more than one maintenance release behind the highest vendor supported level. Where such compliance is not possible, compensating controls must be documented and in place which ensure that the implementation and operation of the system software does not compromise the security of the system. The exception to this is the application of virus definition files, specifically addressed in Section 4.

b) Based on a security risk analysis, all security related patches/fixes must be tested and implemented as soon as possible after vendor release, but not to exceed a period of 90 days. Functional testing must be performed to ensure that the security services and mechanisms are complete and consistent with the documentation, and that other security controls are not compromised by the changes.
c) A change control process must govern all security software updates.
d) All appropriate documentation must be updated upon the completion of each change.

# 3.0 NETWORK SECURITY STANDARDS

**Purpose**

To state the security standards that support the protection of SDLC's distributed networks.

**Scope**

These standards apply to all SDLC computer systems, networks, and devices connected to them, and to their use by both SDLC Staff and approved non-SDLC Staff.

The information contained in this section is intended to supplement the standards already specified in the SDLC Standards of Internal Control, SDLC Data Network Architecture, SDLC Communications Distribution System and other sections of this document. While the prevalent technology is TCP/IP, the intent is to generalize the principles to standards applicable to all proprietary architectures (e.g. SNA).

All facilities at or connected to SDLC must meet the requirements established in Section 2. Any exceptions are noted within the applicable subsections of this section.

**Background**

Due to the growth of internet-worked and remotely accessed systems, data is often distributed between mainframe computers, file servers, workstations and personal computers. Each of these when connected, is considered to be a network node. By definition, a network is an arrangement of nodes and the branches connecting these nodes. Network nodes include any network-connected device, such as firewalls, routers, gateways, network monitors/managers, hubs and concentrators. These devices are also considered network hosts for purposes of these standards.

Data transmitted between network nodes is exposed to more risks than information stored and solely processed in a single computer. While data center environments are vulnerable to accidental or malicious security breaches, data in distributed systems is vulnerable because of the complexity of controls administration and difficulties in maintaining accountability. Data on distributed networks is also vulnerable to tampering with communications circuits and network equipment, and thus must be protected from interception, misrouting and sabotage.

SDLC has little control over telecommunications carriers that are entrusted with the transmission and security of SDLC information. Therefore, systems designed to distribute data between two or more computer systems require special control considerations to ensure confidentiality, integrity and adequate audit trails.

Section 3.0 includes the following subsections:

| | |
|---|---|
| Subsection 3.1 | Network Management Standards |
| Subsection 3.2 | Dial-in and Dial-out Access |
| Subsection 3.3 | Authentication and Encryption |
| Subsection 3.4 | System Penetration Testing |
| Subsection 3.5 | Web Commerce Security |
| Subsection 3.6 | External Connections |

## 3.1 Network Management Standards

Security standards exist for managing SDLC networks just as standards exist for managing SDLC Information. The same fundamental principle applies: perform a risk analysis comparing potential losses of the data with costs associated with the evaluated security options. This subsection describes the standards for the following:

Routers, Bridges and Gateways
Network Tier Management
Connectivity

**3.1.1 Routers. Bridges and Gateways**

Routers, bridges and gateways represent points of access between networks. These devices do not contain mass storage, but do represent points of vulnerability, particularly to unauthorized access or denial of service. Since routers, bridges and gateways may possess little in the way of logical access controls, physical security becomes extremely important. Control of changes to the access control lists (ACL's) on routers, bridges and gateways is central to the secure operation of the network.

a) Routers, bridges and gateways must be placed in a physically secure and locked environment, per Section 6.2.
b) Access controls (ACL's) must be documented and managed using a documented change management process.
c) Custodians must establish procedures for the review of ACL's. The process for review must be based on the sensitivity of

connections at each of the points. An independent reviewer must review ACL's, at a minimum annually, to ensure that the need for the specific ACL's still exists and that unapproved or undocumented changes have not occurred.

#### 3.1.2 Network Tier Management

The SDLC data network is defined as a three-tier system.

- Tier One is the SDLC Wide Area Network (WAN) that is managed by or approved by SDLC Corporate Telecommunications.
- Facility Backbone Networks (FBNs) are defined as Tier Two. FBNs connect LANs to the WAN, and are managed by sectors or groups. Campus and metropolitan area networks (MANs) fall into this category.
- Local Area Networks (LAN's) are Tier Three networks. LAN's may be managed by departments or by an information technology department, at the discretion of the Information technology manager.

a) A system of assigning addresses must be used for all supported network protocols. The system must be uniformly supported and administered throughout SDLC.
b) Sector/group Network Information Centers (SNICs) must work in cooperation with the SDLC Network Information center (MNIC) to administer and maintain unique addressing for all communication protocols.
c) A network inventory of connections must be created and maintained by each facility backbone network organization. (SIC).

#### 3.1.3 Connectivity

SDLC's goal is to provide maximum connectivity between various network nodes while continuing to protect SDLC's information assets and resource availability. An internal network (intranet) is made up of nodes which are all operated under SDLC's supervision. An external network is made up of non-SDLC nodes. An external network is assumed to be a higher threat environment than an internal network, with the highest level of threat being represented by a direct Internet connection. Routers, gateways, switches and bridges connect two or more networks together. When used to isolate networks with dissimilar security policies, these devices are referred to as firewalls. Firewalls make it difficult for attackers to jump from network to network.

The following standards govern connections between networks.

a) A firewall must be maintained between the internal network and any non-SDLC entity. This includes, but is not limited to strategic partners, customers, vendors, joint venture partners, value-added networks (VAN's) and other service providers. See Section 3.6 for more specific requirements.
b) Local management must approve each LAN and FBN connected to the SDLC WAN.
c) Where subnets contain hosts or network traffic that is particularly sensitive or critical, as determined by local management and information security staff, appropriate controls must be documented and installed at the connection point. For example, an internal firewall might be used to isolate a research laboratory, or router access controls might be used to limit accessibility to a subnet operating production equipment.

## 3.2 Dial-in and Dial-out Access

This section describes the standards for dial-in and dial-out access controls.

#### 3.2.1 Dial In

a) Dial-in access to the SDLC data network is prohibited except for incoming facsimile transmissions..
b) A modem must not be set to auto-answer unless:

- the modem is isolated from all other systems and networks, and the associated system contains information no more sensitive than SDLC General Business information, and
- the modem is configured for only facsimile transmissions.

c)

#### 3.2.2 Dial Out

a) Dial out connections are prohibited except for outgoing facsimile transmissions.
b) A modem used as described above must meet the following conditions:
    - The modem is isolated from all other systems and networks, and the associated system contains information no more sensitive than SDLC General Business information, and
    - The modem is configured for only facsimile transmissions.

## 3.3 Remote Network Access

Remote network access, while convenient to the user, is extremely dangerous to the company. Remote network access must be used with care and only as necessary. This section describes the controls for the following types of remote access:

- Web Based Email access
- VPN network access

#### 3.3.1 Web Based Email access

Web based email access to the SDLC email system is permitted through a web browser under the following conditions:

a) The user is a SDLC employee authorized to access the email system remotely,
b) using a SDLC resource (e.g. a laptop or computer) and
c) conforms to the criteria in Section 5.1

#### 3.3.1 VPN network access

Remote access to the SDLC corporate network is permitted through a Virtual Private Network (VPN) under the following conditions:

a) The user is a SDLC employee authorized to access the network remotely, and
b) Is using a SDLC resource containing a VPN client with two factor authentication and
c) Has a Confidential access level clearance and
d) The client system accessing the SDLC network is not concurrently connected to any other network.

Any data retrieved via remote access must be treated as Confidential Proprietary and protected as such. In no instance is the retrieval personally identifiable data such as personnel or client data permitted.

## 3.4 Authentication and Encryption

Authentication is the means to verify that someone who identifies himself is indeed who he claims. Different methods of authentication are used in varying environments, including passwords, tokens, biometrics, or cryptographic keys.

There are at least two cases when network encryption is desired: to protect password transmission and to protect other proprietary data while being transmitted across a network. Several methods of cryptography exist: one-way, symmetric, and asymmetric encryption.

One-way encryption algorithms are primarily used for protection passwords.

The conventional symmetric method, exemplified by the DES (Data Encryption Standard), uses the same key to both encrypt and decrypt information. This method is only beneficial in situations where the exchange of keys is a small risk.

Asymmetric encryption methods, such as public/private key, provide the best technology for authentication and digital signatures. Public/private keys are based around the concept that one key is used to encrypt information and a different key is used to decrypt it.

#### 3.4.1 Password Encryption

Password authentication relies on cryptography for adequate protection. Basic password standards are discussed in Section 2.2. Password encryption standards in this section are intended to supplement the information contained in Section 2.

a) Passwords must be encrypted during network transmission.
b) Passwords must be stored in encrypted form.
c) All authentication passwords must be stored in encrypted form. Passwords stored on the host computer containing the account being protected must be stored using one-way encryption (hashing).
d) Encryption must be used in compliance with local legislation.

#### 3.4.2 Data Encryption

a) SDLC Registered Secret Proprietary and higher information must be encrypted end-to-end when transmitted.
b) All information transmitted by radio must be encrypted.
c) SDLC Internal Use Only and higher data must be encrypted when sent outside a SDLC facility.
d) Message compression techniques (e.g. PKZIP) must not be used as a means of security.
e) External connections between SDLC facilities must be encrypted.
f) Dedicated communication circuits in countries that prohibit the use of encryption must use cable systems with the maximum amount of protection possible.
g) Sectors/Groups, in conjunction with the Information Security Council, must approve

encryption mechanisms.

#### 3.4.3 Key Management

a) Keys must be distributed using encryption mechanisms approved by Sectors/Groups in conjunction with the Information Security Council.
b) Public/private keys must be created, assigned, and distributed using a documented procedure that can be audited.

c) Any symmetric cryptographic key used by one communicating pair must not knowingly be used between any other communicating pair.
d) The major encryption keys for link encryption devices must be changed from the default values at the time of equipment installation.
e) Link encryption keys must be configured to change as often as possible, not to exceed seven days.
Audit trails must be used to record the distribution of encryption keys. The log must identify the manager responsible for key distribution.
f) Encryption key changes require the documented approval of at least two supervisory individuals.
Access to physical keys for encryption hardware must be limited to authorized staff.

## 3.5 System Penetration Testing

SDLC has a large investment in proprietary information stored on, processed by, or accessed via a wide range of information systems and network equipment. These systems are often protected by software means, such as the use of login IDs, passwords and access control rules.

This section describes under what conditions sanctioned penetration tests may be conducted, who must approve the testing, who may conduct the tests, who must be notified, and who gets the results of the tests.

**Definitions:**

***System Custodian:*** The SDLC or approved non-SDLC staff LAN or system administrator who is directly responsible for the system to be tested.

***Testing Authority:*** The person who authorizes testing of security controls. He or she may delegate that responsibility as described in Section 6. By definition, the following people may authorize tests:

1. The system owner (for his or her system only)
2. A business unit's Director of Information Technology (for all systems in his or her scope of authority)
3. A business unit's financial controller (for all systems in his or her scope of authority
4. The corporate or sector/group information security manager.
5. A corporate Senior Audit Manager

#### 3.5.1 Conditions for Penetration Testing

a) Sanctioned penetration testing may be performed only for the following reasons:

- To verify that existing security controls are functioning, including the system custodian's ability to detect attacks
- To confirm the existence of a system or control vulnerability

b) Sanctioned penetration tests must be pre-approved in writing by a testing authority. Tests must be approved by the system owner and executed by or under the supervision of the system custodian unless:

- The testing is part of an audit, and included in the audit scope
- The testing is necessary for the investigation of an incident
- The system custodian is being tested to see if he or she will detect and respond to an intrusion

c) System owners must be referred to a testing authority that shall review the request and either sanction testing or reject the request. This may include testing without the knowledge of the system owner or system custodian, as explained above.
d) Only the above-referenced system owner or testing authority may sanction testing. All other test approvals are prohibited.
e) The testing authority may delegate, to qualified SDLC staff, the authority to sanction testing, and/or to select the personnel to perform tests.
f) A bonded outside contractor may be used for sanctioned penetration tests only if the contractor is nominated using the WWCFP A-6 procedure, signs a non-disclosure statement, and is approved by the Corporate Director of Information Security and Risk Management or a Corporate Senior Audit Manager
g) Results of penetration tests shall be treated as SDLC Confidential Proprietary information. Refer to Policy SOP (POP Section 1.3.1) for information on storage, processing and handling requirements.
h) Penetration testing tools shall be restricted to those individuals with a legitimate need for access.
i) Care must be taken so that the tests do not adversely affect the operation of the system under test, or the integrity,

confidentiality or availability of data.

j) Penetration attempts may trigger intrusion detection mechanisms; therefore, prior to the initiation of testing, the sector/group information security manager must be notified as to the conditions and intent of tests.

k) If any specific controls are identified as inadequate or needing corrective action, the tester or testing authority must notify the system owner, system custodian, data owner, and data custodian, as appropriate. The notifications and responses must be documented. For example, if a weak password is identified the user/account owner must be asked to change it. If a procedure is faulty, the custodian of that procedure must make revisions.

l) Information about a deficiency must be restricted to those directly responsible for determining and implementing the corrective action.

## 3.6 Web Commerce Security

SDLC has had Internet web presence since 1998. At first, most of SDLC's Internet web content was relatively small, static and time insensitive. Today, SDLC's Internet web presence has a growing need to provide large amounts of dynamic and real time information to the end user. In the past, when there was a need for access to such timely information outside of SDLC, data had to be replicated from an internal data source to a computer outside of the SDLC network. Data mirroring and replication techniques were never intended to support demands for interactive real time information, and quickly proved to be insufficient.

The Firewall Task Force developed the web commerce security architecture to allow external SDLC web servers access to SDLC's internal data while maintaining the integrity and security of the nodes and data on the SDLC network. The need to access dynamic or otherwise real time data from the original source is now possible within this architecture.

Static web content and less time sensitive information on SDLC's external web servers will continue to utilize the staging and releasing of documents through existing replication and mirroring techniques.

**Scope**

This section applies to any SDLC equipment supporting web commerce.

This section contains the following subsections:

- Reverse Proxy Security Architecture
- Web Commerce Server Security Requirements
- Internal Data Store Security Requirements

**3. 6. 1 Reverse Proxy Security Architecture**

Each component of the architecture must be viewed as being a part of the Internet firewall. The SDLC network, the computers on the network and the applications on the computers accessed must be well managed to ensure a secure environment. Figure 1 depicts the overall reverse proxy security architecture. The notes explain where the requirements apply and which components must satisfy them.

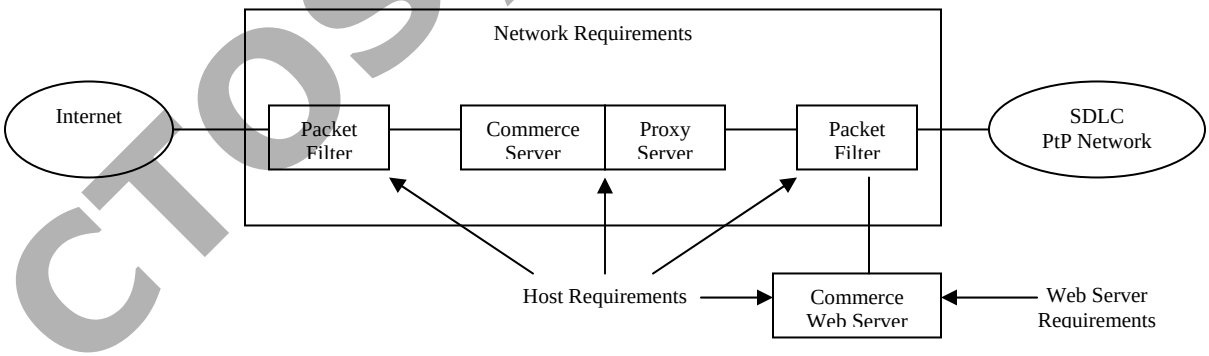


**Figure 1**

The reverse proxy is extendible, in that the web commerce server does not have to reside were the Internet firewall resides. The remote reverse proxy architecture is depicted in Figure 2.

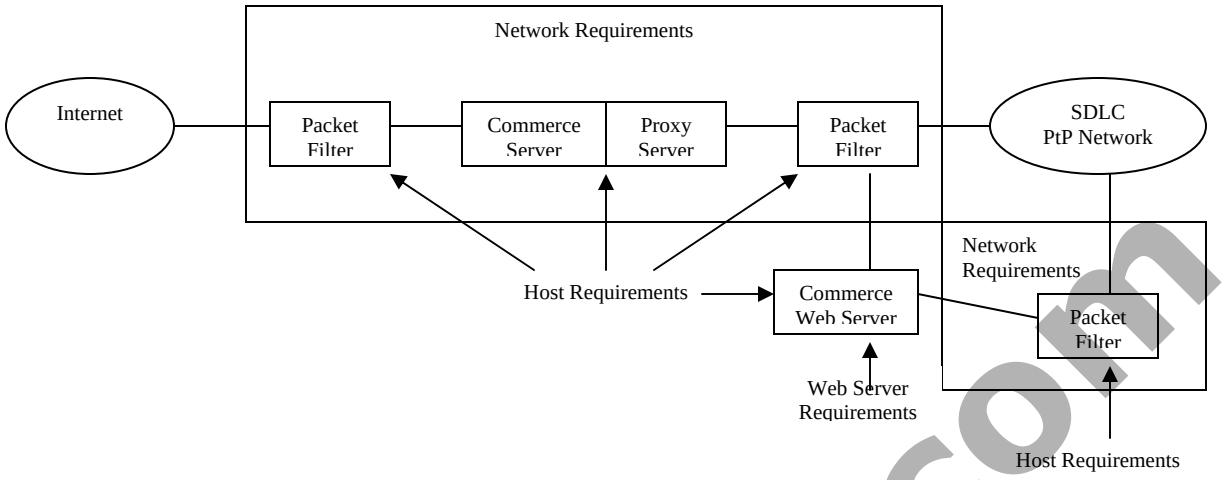


**Figure 2**

Note an additional packet filter has been added to the remote architecture in Figure 2. This new component must meet both the networking requirements and host requirements, and by doing so it safely and securely extends the reverse proxy architecture anywhere within the SDLC data network.

Figure 3 demonstrates how data flows through the architecture. The data is decrypted and passed to the reverse proxy were it is inspected and verified as an authentic http protocol instruction. The reverse proxy then establishes the appropriate connection to the commerce web server and begins to forward all legitimate http traffic between the end user and the server. The reverse proxy can be configured to communicate with the server via http (unencrypted) or HTTP.S/SSL (encrypted). The commerce web server is then permitted to interact with the internal data store using the appropriate database or other data retrieval protocols supported by the architecture.

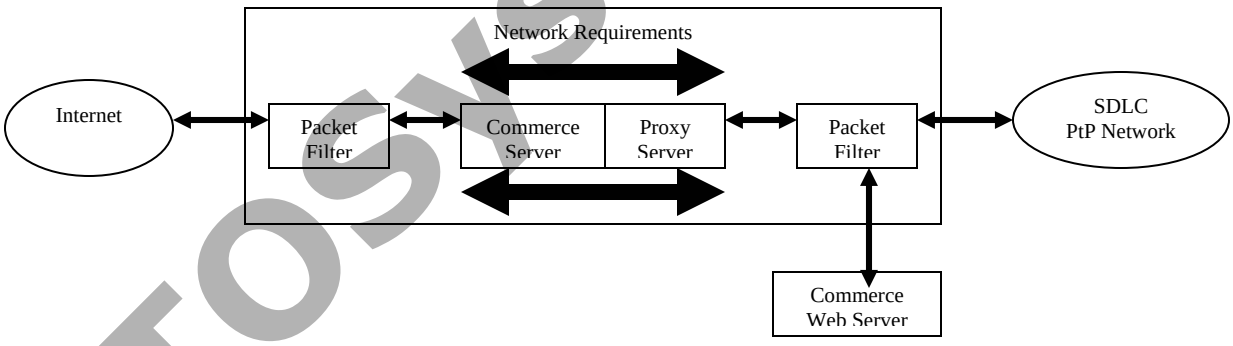


**Figure 3**

a) Approved security measures must be implemented at each layer of the architecture.

- The boxed area in Figure 1 represents which components must satisfy the networking requirements. Complete requirements are in Section 3.7.2.
- Host requirements can be found in Section 3.7.3.
- The security requirements of the internal data store are in Section 3.6.3.
- The commerce web server (the actual server which the end user interacts with) must meet the web server requirements (see Section 3.6.2) in addition to the host requirements.

b) Network connections must be initiated by end users using an SSL capable browser.
c) Inbound connections used to retrieve SDLC data must use port 443 only.

#### 3.6.2 Commerce Web Server Security Requirements

a) A change management process must exist and changes to the web commerce systems must be documented.
b) A configuration management and change control process must be implemented for web server content.
c) There must not be any development, testing or web content building on the production system.
d) The commerce web server must limit its functions to validating user/application data (for format and syntax only) and to making requests of the internal data store server.
e) The commerce web server must not act as a proxy.

#### 3.6.3 Internal Data Store Security Requirements

An internal data store is an internal SDLC host whose data is accessible from a device that is considered part of the web commerce security architecture.

a) The internal data store (database server) must implement controls that limit the amount of data delivered, or actions taken, to only those actions that are approved. For example a legacy SOL server must not respond to general queries from the web commerce server, but must only respond to expected, restricted queries (e.g. no wildcard searches, get-next loops, etc.).
b) The internal data store must log all accesses/service transactions it performs. The logs must contain sufficient level of details to provide an audit trail (e.g. the query/action it received, identity of the user, a time and date stamp, and the end result of the query/action).
c) The internal data store must guarantee that access to, and actions on, the specific data are explicitly approved for each user making a request.

## 3.7 External Connections

An external connection is any connection between a SDLC network and a non-SDLC network. External connections are difficult to secure and require a very substantial investment in hardware, software and administrative time. For example, log files and operating system security issues must be monitored continuously, and fixes implemented immediately. Potential intruders probe SDLC's Internet connections for weaknesses every day. New types of attacks occur within several hours of a vulnerability being discovered and publicized on the Internet. Managing an external connection requires advanced skills, state-of-the-art technology, and a strong commitment of time and resources. Therefore, a security boundary must be maintained between the SDLC data network and external networks.

**Scope:**

Any connection from a SDLC network to a non-SDLC network.

This section contains the following subsections:

- The Network Interconnection Architecture
- Network Security Requirements
- Host Security Requirements

#### 3.7.1 Network Interconnection Architecture Requirements

**Definitions** :

Filter: Controls network traffic in OSI protocol layers 1-4.
Proxy: Controls network traffic in OSI protocol layers 5-7.

a) The security standard for external to internal connections must be designed around a proxy architecture approved by the Information Security Council and group/sector information security staff.

1 Every component must have the ability to log at the protocol layer it is filtering.
2 A minimum of two separate hosts is required. The external proxy and filter may be combined on one host and the internal proxy and filter may be combined on one host.
3 Proxy #2 is optional for TCP services with the source internal and destination external SMTP/NNTP).
4 The proxy can be single or dual ported, with dual ported preferred.
5 All hosts must be backed up locally or not at all. Backups must made on nonrewritable media. Remote backup is not permitted.
6 Filter #2 must maintain session state information to prevent exploitation of vulnerabilities associated with dynamic reply ports.
7 Filter #2 must maintain session logs.
8 All devices must have two-factor authentication for administration.

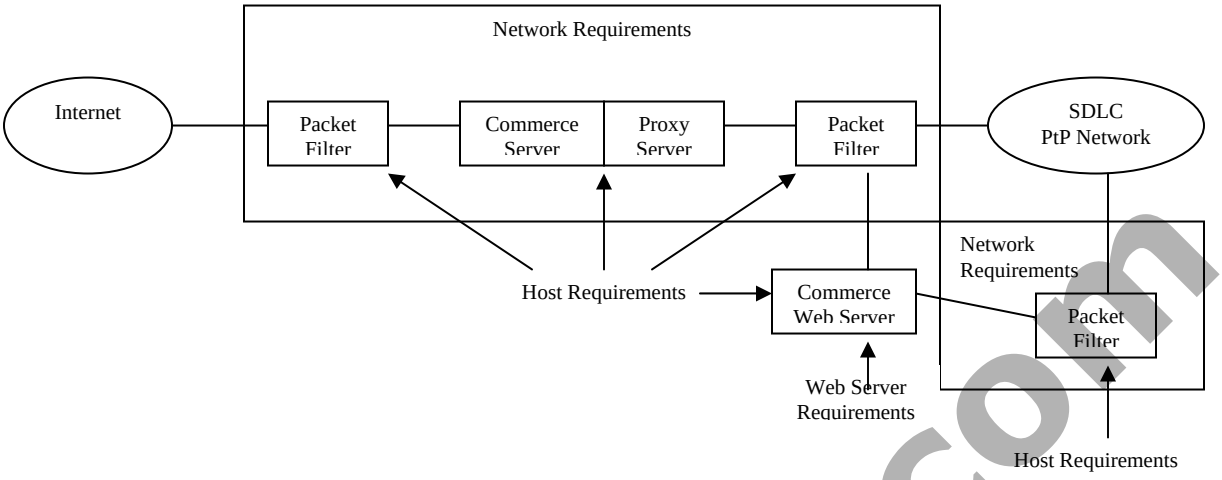


**Figure 4 – Network Interconnection Architecture**

b) The text below must be displayed to interactive (e.g. http, telnet) users connecting from the SDLC network to the Internet before access is granted. The items must link to the respective policy and guideline.

**Appropriate Use Reminder**

SDLC encourages the use of the Internet for business and management-approved purposes, however any breach of the SDLC policy SOP -- Appropriate Use of Computer Resources will be vigorously pursued. Please read the Appropriate Use Guideline for examples of appropriate and in appropriate activity. Always:

- Use the Internet only for business and management-approved purposes
- Protect all intellectual property rights and copyrights
- Comply with security rules and laws, including import/export
- Communicate politely --you are representing SDLC
- Avoid offensive graphics and illegal activity

The details of all sites you visit while accessing the Internet will be monitored and may be checked to ensure compliance with policy. Thank you for your understanding and cooperation.

**3.7.2 Network Security Requirements for External Connections**

a) Network security and administration controls (e.g. access, firewall, monitoring, operations, configuration files, and time zone) must be fully documented. The documentation must include high-level network diagrams with text descriptions.
b) A packet filter must be used to limit, control and protect all hosts/servers in the architecture. Access controls must be put on the packet filter to enforce and compliment the host and application control. For example, e-mail connections between e-mail relay hosts must be specifically permitted, while the packet filter must deny all other services.
c) An application proxy must be used to validate the application protocol for any service that passes into or out of the SDLC network.
d) Network controls must be in place to reject invalid, spoofed, or replayed packets.
e) Only necessary, approved "securable" services must be allowed. See 3.6.4 Application, Service and Protocol.
f) An approved network vulnerability-testing tool (e.g. Internet Scanner) must be used to verify the controls in place for the firewall hosts. Changes in the output of the testing tool since the previous run must generate an alarm. This tool must be run after each configuration change, or at least monthly.

**3.7.3 Host Security Requirements**

The term "host" refers to the firewall device(s), web server(s), and internal/legacy data server(s) accessible from an outside network via the web commerce proxy.

a) Each host must have controls that determine which of its services may be used. Only necessary services may be active.
b) Appropriate authentication must be implemented based on a risk assessment. For example, when the need for non - repudiation exists, approved controls must be implemented to support this.
c) Each host must log all network connections to it. The logs must contain the source address, a time and date stamp, and pertinent information about the service request or network activity.
d) No application proxy (e.g. http web proxy) is permitted to run on the host.
e) Approved intrusion detection tools must be active on the hosts to monitor for unusual activity, connection requests and authentication failures. The tool must have configurable thresholds, alarm generation facilities, and be able to stall or stop attempted break-ins. Discrepancies must be investigated when found.
f) Approved integrity tools must be active on the hosts. The tools must be able to check and report unauthorized changes to binary and configuration files. The minimum checks are boot files, the kernel, the password file or registry, services, network configuration files, system services binaries, and host configuration files. Discrepancies must be investigated when found.
g) An approved system configuration-checking tool must be run monthly. The minimum checks are boot files, kernel, password file, network configuration files and host configuration files. Discrepancies must be investigated in a timely manner.
h) All unneeded files and services, including applications and compilers, must be removed. Executables must be statically linked; dynamic run-time libraries must be removed. Anything that is not needed for the host to function must not be on the machine.
i) Appropriate authentication and encryption must be in place to protect the host's data, sensitive and critical information.
j) All interactive privileged network logins must use two-factor authentication, and must not be allowed via network segments susceptible to session hijacking or spoofing.
k) With the exception of administrative accounts, no user accounts may exist on the hosts and network devices.
l) A configuration management process/change control process must be implemented for configuration and executable files. There must not be any development or testing on the production system.
m) The host must use an automated method to synchronize its clock with an authoritative SDLC time server.
n) Self-assessments or independent audits must be performed every six months. A failure on any control issue must immediately be corrected and followed by a thorough security review. The underlying cause of the failure must be identified and controls put in place to prevent future recurrences.

#### 3.7.4 Application, Service and Protocol Standards

Specific standards for applications, services, and protocols that are supported through a firewall must be determined by consensus of a "peer review board" made up of group/sector information security and networking staff. These standards must be documented.

# 4.0 COMPUTER SYSTEMS SECURITY STANDARDS

**Purpose:**

To secure all computer systems and the business information stored on them by appropriately protecting the information from unauthorized user access, intentional or inadvertent disclosure, loss, modification, destruction or copying.

**Scope:**

These standards apply to all computer system hardware platforms used in the execution of SDLC business. Examples include, but are not limited to all computer systems used in manufacturing, engineering, office and home environments.

The information contained in this section is intended to supplement the standards already specified in the SDLC Standards of Internal Control and the SDLC Data Network Architecture documents.

All SDLC computer systems must meet the requirements already established in Section 2 and 3, and the SDLC SOP. Any exceptions are noted within the specific subsections of this section.

This section includes the following subsections:

| | |
|---|---|
| Subsection 4.1 | Information Security for Computer Systems |
| Subsection 4.2 | Virus Control |
| Subsection 4.3 | License Compliance |
| Subsection 4.4 | Mobile Computing and Telecommuting |
| Subsection 4.5 | Personal Digital Assistant Security |

## 4.1 Information Security for Computer Systems

Information security is the joint responsibility of the computer system user, the user's manager, and the custodian of the equipment.

#### 4.1.1 Access Control

a) Each computer system must have approved security software installed that requires a password AND/OR a secure authentication mechanism that meets SDLC standards.
b) Protection mechanisms must be in place to prevent direct access to data on the fixed disk or from removable media when booting. An authorized exception would be when service personnel follow approved service procedures with the permission of the user or with management approval to service a computer system.
c) Access controls must allow password configuration to meet the standards of Section 2.
d) Where secure authentication mechanisms are used, they must require a minimum of two-factor authentication to meet the standards of Section 2.
e) The access control system must require a unique login ID and password for each user of the system in accordance with Section 2.
f) The computer system must have a timed lock-out/screen blanking mechanism, which automatically engages after no more than ten minutes of inactivity, or when manually invoked. When activated, it must prompt for a password that preserves the integrity of work
in progress.
g) The number of system logon entry failures must be limited to three. A time delay or system lockout must be inserted after the third invalid attempt. It is recommended that the delay be set to a minimum of two minutes, if configurable in the software. The security objective is to block automated password guessing.
h) The access control system must be configured to provide an audit trail for preventative/detective measures in case a computer system is compromised.
i) The access control system must be configured to allow access by an authorized administrator.
j) Dial-in/Remote access is only allowed through a SDLC approved dial-in/remote access system in accordance with SOP and Section 3.

#### 4.1.2 Shared Computer Systems

The following standards apply to all computer systems that are used by more than one user.

a) The access control method must provide for the registration and tracking of each user's logon activities.
b) User data and/or business applications must be protected by access controls to segregate access to them among users authorized to use the computer system.
c) Users cannot be their own administrators unless specifically documented and approved by local management. If there is a legitimate business need for the user and the administrator to be one and the same, the following standards must be adhered to:

   I) A documented process must be in place to independently review the system security configurations and ensure that all security software, including anti-virus software signatures, are up to date. This must occur at a minimum quarterly.
   II) Administrator accounts must only be used when specifically required to perform administrative actions not permitted under their standard user account.
   III) The administrator account password must be changed every thirty days in accordance with Section 2.

#### 4.1.3 Information Security

In accordance with SDLC's POPI standards (Section 1.3.1), the control requirements for each information sensitivity level are described in the following table:

| Classification of Information | Control Requirements |
|---|---|
| General Business Information (GBI) | Controls exist only to prevent unauthorized changes to data and to the operating system. Unrestricted read access is granted to CGB data residing on the host. |
| SDLC Internal Use Only (IIUO) | In addition to the requirements for SDLC General Business, controls must exist which establish individual user accounts and passwords. Read and write access is granted based on the need to know. |
| SDLC Confidential Proprietary (ICP) | In addition to the requirements for SDLC Internal Use Only, an audit trail must be created, protected and archived for at least one year. This audit trail must record all security sensitive events, including:<br>• Logons<br>• Logoffs<br>• Failed Logons<br>• Password changes<br>• Addition of authorized users<br>• Deletion of authorized users |
| SDLC registered Secret Proprietary (IRSP) | In addition to the requirements for SDLC Confidential Proprietary, CRSP requires documented procedures to record all access and use encryption as detailed in Section 3.3 of this document. |

a) Responsibility for each computer system on the SDLC network must be assigned to a custodian. This person is responsible for the security of the computer system and any data residing on it.
b) The custodian of the computer system is responsible for determining the highest level of information requiring protection and for establishing controls which support the security requirements of that level of information. Other users having access to the computer system must be advised of the data protection level of the device.
c) SDLC Registered Secret Proprietary information residing on a fixed disk must exist in encrypted form to avoid compromise by unauthorized persons as identified in Section 3.
d) SDLC Confidential Proprietary information stored on a fixed disk on a computer system shared by more than one person must be protected by additional access controls other than those used to gain access to the basic computer system. Examples include individual access permissions configurable in an NT or UNIX operating system.
e) Removable electronic storage media (e.g. diskettes, CD ROMS, DVD, etc.) must be clearly labeled and secured in a locked desk or filing cabinet at the end of the workday in accordance with the POPI guidelines set forth in SOPs.
f) External electronic storage media must be secured at the end of the workday.
g) When not in use, removable electronic storage media containing SDLC Confidential Proprietary or higher information must be clearly labeled and secured in a locked desk or filing cabinet.
h) When disposing of any information classified as SDLC Confidential Proprietary or higher, that information must be overwritten or the media reformatted to ensure it is unrecoverable, or the media physically destroyed.

#### 4.1.4 Hardware Maintenance

These standards apply to any maintenance that is performed to hardware, software or computer system equipment. It is recommended that hardware and software maintenance contracts be in place, but this is a business decision.

a) All SDLC data must be overwritten or the media reformatted to ensure it is unrecoverable on a rented, leased, or SDLC-owned computer system when sent out for service and repair unless covered by a non-disclosure agreement.

b) When data exists on external drives being serviced, it must be removed, reformatted or overwritten to ensure it is unrecoverable.
c) All non-SDLC staff maintenance personnel must sign a non-disclosure agreement and otherwise comply with the provisions of WWCFP A-6. Any non-SDLC staff maintenance personnel who do not comply must at all times be escorted and closely monitored while they are in a SDLC facility, unless they have a non-escort badge and a specific SDLC manager assumes accountability for their actions.
d) Any magnetic media used for troubleshooting or diagnostics must be available for SDLC employees to check for the presence of unauthorized data files, software, or viruses.
e) Remote diagnostic links to non-SDLC equipment are not permitted.
f) Malfunctioning parts or circuit boards must be replaced with factory-fresh or factory-repaired components. If non-volatile components are involved, they must be erased or removed and destroyed.
g) After maintenance has been completed, the custodians must immediately change all passwords that may have been compromised and scan the system for viruses.
h) If the drive has critical data that needs to be recovered, it must be sent to a data recovery service agent where applicable non-disclosures have been signed.
i) If the drive contains SDLC Registered Secret Proprietary data, the SDLC staff member who has authorized access to the data must accompany it at all times.
j) If the drive has become inoperable and the data unrecoverable, the media must be physically destroyed.

#### 4.1.5 Hardware Reassignment and Disposition

The following standards apply to any computer system or peripherals that are reassigned to a different individual or department, returned to lessor, salvaged, or placed in storage.

a) All removable media (e.g. diskettes, cartridges, CD's, DVD's, and tapes) must be removed.
b) All SDLC data must be overwritten or the media reformatted to ensure it is unrecoverable This includes external drives that will remain with the computer system.
c) All SDLC-licensed software must be removed from a rented or leased computer system prior to its return to the supplier.
d) When a computer system is transferred between individuals, its data must be overwritten or the media reformatted to ensure that no confidential data is compromised and no data remaining on the computer system opens the potential recipient to issues of inappropriate usage.
e) Circuit boards with non-volatile read/write data memory must be erased or removed.
f) Carbon ribbons and thermal cartridges must be removed from fax machines, printers, and other devices before equipment is reassigned. One-time-through carbon ribbons and thermal cartridges removed from printers and fax machines must be discarded in accordance with the POPI classification associated with them.
g) All paper products must be removed from all printers and fax machines.

## 4.2 Virus Control

Viruses are unauthorized programs that can propagate themselves into programs or data and cause destruction or damage to computer system programs, data or networks.

Virus detection software running in "active" mode refers to software that performs its desired function automatically. With active virus detection software, computer systems can continually monitor themselves for the presence of virus-like behavior. and scan floppies and external media when first mounted into a computer system before allowance is given to read or execute data on them.

It is the computer system user's responsibility to ensure the following requirements are met:

a) All computer systems used for SDLC business must have virus detection software installed with active mode enabled. At this time, virus detection software is not available for mainframe, UNIX, or PDA systems, so they are exempt until such time that approved software exists. When using emulators on operating systems that allow emulation mode of other operating systems (e.g. SoftWindows, WinDD, MAE, etc.), anti-virus software is required.
b) All computer systems must be configured to scan all removable media when inserted into the system.
c) All virus detection software must have the latest version of virus definitions applied. Updated definitions are currently available monthly from anti-virus software vendors.
A full virus scan must be performed each time virus definition files are updated.
If virus detection software running in active mode is disabled at any time (e.g. to install software that required virus software be disabled), then full scans must be performed daily until the active mode is re-enabled.
d) All software and data must be scanned before it is loaded onto any SDLC computer system, and a full scan must be performed after it has been loaded. This is necessary because there are some situations where compressed files do not get properly scanned before they are decompressed and installed.
All software from public or private sources, including but not limited to the Internet, electronic bulletin boards, etc., must be scanned before use.
e) Upon the discovery of a suspected virus that cannot be repaired with the installed anti-virus software, the computer system user must:
    - Cease all operations
    - Notify the responsible computer system support personnel

- Document conditions and status of the environment
- Report the occurrence to the appropriate support or Information Security Personnel.

## 4.3 License Compliance

Changes in license agreements and legislative and contractual requirements have created a requirement to implement a more dynamic approach to ensuring license compliance. Licensing, as well as legislative requirements, vary from country to country. The penalty for not being compliant with licensing is far greater than the cost of being legal. Responsibility for complying with software license agreements belongs to each individual computer system user or custodian. Software is licensed in several fashions, each with slightly different requirements for adhering to licensing agreements. The purpose of this section is to identify the security requirements for license compliance. If unsure of compliance, users should contact their LAN Administration group.

#### 4.3.1 Software Usage

a) All software that is approved and purchased must be used in accordance with the terms of the software licensing agreement for the product.
b) Unlicensed software must not be used on any computer system. In the event unlicensed software is detected, a legal copy must be purchased immediately or the software must be deleted.
c) Software is intellectual property, which is protected by copyright laws. Software must be protected from reproduction in strict accordance with the terms of license agreements.
d) A documented process must exist for performing regular software audits to reconcile software licensing. At a minimum, audits must be performed across all SDLC computer systems on an annual basis.
e) Where master or site license agreements are not in place, copies of the original software media, license certificate, invoice, manuals, and/or purchase order must be retained as proof of licensing. Local management must decide whether the licenses are retained departmentally or by individual users.

#### 4.3.2 Concurrent Licensing

Concurrent licensing allows SDLC to make a designated number of licenses available to unlimited users in a shared server environment, as long as the maximum number of concurrent users executing the software at anyone time does not exceed the concurrent number that is licensed.

a) When concurrent licensing is deployed, a mechanism such as metering software or license servers must be in place to restrict the number of concurrent users to the maximum number of licenses authorized.
b) The implementation of concurrent licenses must ensure that the only nodes that can access licenses are within the physical boundary specified in the license agreement.
c) The method of implementation must be carefully reviewed to ensure that when the software is not executed, no parts of the software remain loaded in memory on the computer system, such as a dependent TSR, VxD, or Wrapper.
d) A license agreement must be on file that clearly states the maximum number of concurrent licenses allowed.
e) When concurrent licensing is deployed and "Suite Support" is required (Microsoft Office, Lotus Suite, etc.), metering software must accurately monitor and account for individual products within the Suite.

#### 4.3.3 Individual or Named User Licensing

Individual or named user licensing is software that is licensed to a particular user or computer system and are generally required for applications that have "individual data" or individual use needs, such as an E-mail package, personal calendar package, etc.

a) When individual licensing is deployed, each user of the program must purchase a separate license to run the software.

#### 4.3.4 Node-Based Licensing

Node-based licensing requires that software only be run from a specific node on an individual basis. An example is an engineering application called PSPice.

a) Node-based licenses can only be installed on a shared server within SDLC if there is an active metering program (e.g. FlexLM) to limit license usage to the nodes specified in the agreement.

#### 4.3.5 Server-Based Licensing

Sever-based licensing allows a defined maximum number of users accessing a server to execute an application. An example is Microsoft Exchange.

a) In server environments where licensing is based on a designated number of connections, a process must be in place to ensure that accesses to any server-based licenses match the number of server licenses allowed.

#### 4.3.6 Evaluation or Demonstration Software

Evaluation or demonstration software is usually a fully functional copy of new software applications, intended explicitly for evaluation purposes.

a) All evaluation or demonstration software must be removed from active use upon the conclusion of any authorized evaluation period unless purchased or legally licensed for Company use.
b) The person installing the evaluation software must retain proof of the length and conditions of the agreement through the duration of the evaluation period.
c) Evaluation software must not be used for production work unless specifically authorized in the vendor agreement.

#### 4.3.7 Shareware/Freeware Software

SDLC discourages the use of Shareware/Freeware software, especially in mission critical environments. In cases where Shareware/Freeware software is used, the following conditions must be met:

a) Most Shareware/Freeware software is copyrighted and most of this software contains a licensing agreement. It is the responsibility of the user to understand and comply with all usage and licensing agreements. Users must recognize that many freeware products must be purchased for commercial use (installation on SDLC computer systems constitutes commercial use).
b) Shareware/Freeware software provides little or no liability protection if software programs do not function correctly and cause havoc on computer systems. This type of software may not undergo formal testing to ensure quality assurance that commercial software products are subject to. To ensure that security and integrity are not compromised, isolated tests must be thoroughly performed before loading this software on any production computer system.
c) Most Shareware/Freeware software is not well supported and therefore would not be recommended for inclusion in SDLC Products. If situations exist which require the use of Freeware/Shareware software in SDLC products, adequate support must be available and license agreements must be carefully reviewed to ensure that they allow for re-packaging or commercial sales.

#### 4.3.8 Licensing Compliance for Second System Use

Some vendors specify that software that is purchased can also be installed on a home or laptop computer system under certain conditions or based on percentage of usage at the office vs. home. The following standards must be followed when installing SDLC-licensed software on a second system:

a) Management must approve the installation of any SDLC-licensed software on multiple systems (e.g. home systems, desktops and laptops, etc.). Usage of the software must be documented and tracked.
b) It is the responsibility of the person installing the software to verify that the installation adheres to the specific license agreement of any product.
c) SDLC software that is installed on any associate-owned computer systems must be deleted upon separation from SDLC or when job responsibilities no longer support the use of it.
d) As software licensing agreements are renewed, home usage or multiple installations must be reviewed and re-evaluated as to their adherence to updated agreements to ensure that the licensing agreement still allows for this type of usage.

#### 4.3.9 Software Export and Import

a) Deployment of an application must be legal within the country where it is being installed. (For example, some countries do not allow encryption products.)
b) The procurement and/or export of software must comply with the governing laws of the country to which it is being exported from.
Appropriate documentation must accompany all software that is moved between countries to ensure no legal issues arise when crossing borders.

## 4.4 Mobile Computing and Telecommuting

This sub-section encompasses any use of SDLC computing resources, including hardware, software, data, printed reports, etc., outside of SDLC physical facilities. This sub-section assumes that all standards applied to SDLC-owned computing resources within SDLC facilities will be applied to SDLC-owned resources outside SDLC facilities, and therefore lists only those additional issues that result from being outside the normal reach of SDLC physical security.

#### 4.4.1 Mobile Computing

Mobile Computing consists of carrying SDLC computing resources out of the facility on a temporary basis to enable productivity while traveling, at a customer site, etc. in the normal course of business. Modularity and large-capacity portable drives make it easy to transport stolen data for access on another computer system.

a) In addition to the normal controls, any data classified CCP or higher on a laptop must be stored in encrypted format.
b) Laptops, modular drives, and removable disks must be kept physically locked up when not in the possession of a SDLC employee.
c) A documented procedure must be in place for security administration (e.g. emergency password changes).
d) When a machine is off-site, there is limited or no access to the normal backup resources of the network. The employee's department is responsible to ensure that backup resources are provided that will comply with the backup requirements in Section 7 of this document.
e) No data classified CCP or higher may opened or viewed in a public area (examples include hotel lobbies, restaurants, airplanes, airports, plazas, parks, convention centers, conferences, etc.)
f) Public and hotel fax machines and printers must not be used for printing documents classified higher than SDLC Internal Use Only unless the recipient is physically present to receive the documents.

#### 4.4.2 Telecommuting

Telecommuting consists of using SDLC computing resources on a permanent or part-time basis working from home.

a) The employee is responsible for the physical security of all telecommuting computer systems.
b) Controls must be in place to ensure that access to SDLC data and software on the computer system is granted only to the employee.
c) A documented procedure must be in place for security administration (e.g. emergency password changes).
d) The employee's department must ensure that backup resources are provided that will comply with the backup requirements in Section 7 of this document.

#### 4.4.3 Occasional Work at Home

Occasional work at home consists of using employee-owned computer systems and/or software at home to avoid being at the office during off-hours. When SDLC information is processed on employee-owned hardware, the employee is responsible for exercising the same precautions as if the information or data was contained on a SDLC computer system for mobile use

a) The employee is responsible for securing hardware, software, and data per SOPs.
b) Records of SDLC-owned software installed on employee-owned computer systems must be kept in the office, accessible to any individual who is responsible for reporting or auditing the information.
c) The employee must comply with the backup requirements in Chapter 7 of this document.

## 4.5 Personal Digital Assistant (PDA) Security

Personal Digital Assistants have gained popularity as a convenient method for storing appointment and address information and carrying it around in a small physical device. As these electronic devices become more prevalent and powerful in their data storage capabilities, information security controls must be implemented for devices storing SDLC data.

Examples of these devices include those running the Windows CE operating system, Blackberry, Visor, PalmPilot, Newton, Sharp Organizer, Psion, etc.

This sub-section assumes adherence to all applicable SOP's and SIC's.

a) PDA's are extremely portable devices and therefore must be more rigorously protected against loss. They must be kept physically locked up when not in the possession of a SDLC employee.
b) In order to protect information stored in the PDA, either password protection, data encryption or ID/password protection is required. A mechanism must also be provided for authorized access to the data stored on the PDA by other than the primary PDA user
c) Remote access capability is provided with many of these devices. To reduce this potential vulnerability for remote access to SDLC's network, approved two-factor authentication must be used. PIN's, ID's and passwords must not be stored on these devices.
d) Many PDA's support the downloading of applications to enhance their functionality. Many of these applications are freeware/shareware as well as commercially available. Proper controls over the licensing of these applications must be in place. Proof of license must be available for audit of all software installed on the PDA.
e) Downloading of files and documents and synchronization of data with desktop computer systems are supported by many PDA's. Controls must be in place to insure the integrity of data transferred. Anti-virus scanning is required for all files downloaded from the PDA to the desktop system.

f) PDA's are subject to audits in compliance with the same standards applied to other computing devices.
g) In most cases information stored in PDA's will be lost if batteries fail. Therefore proper backup procedures must be implemented.

All of the electronic facilities used at SDLC must meet the basic requirements established in the General System Integrity and Security Control standards (Section 2). All exceptions are noted within the applicable subsections.

# 5.0 SPECIFIC NETWORK TECHNOLOGY SECURITY STANDARDS

**Purpose**

To define the minimum-security standards for transmitting messages via electronic facilities such as mail systems, bulletin boards, fax machines, voice mail, and video conferencing equipment.

**Scope**

These standards apply to all of SDLC's computers and networks, including voice and data communications, and their use by both SDLC Staff and approved non-SDLC Staff.

The information contained in this section is intended to supplement the standards already specified in the SDLC Standards of Internal Control.

Four types of networks generally exist: public data networks, intra-enterprise networks, inter-enterprise networks, and value added networks. Briefly, public data networks, such as the Internet, are open to public access from anyone around the world. Intra-enterprise networks only transmit communication within a single company. Inter-enterprise networks provide connections that enable users from different companies to exchange electronic messages. Value Added Networks (VANs) provide additional service beyond the standard transport function.

Section 5.0, entitled Specific Network Technologies, includes the following subsections:

| | |
|---|---|
| Subsection 5.1 | Electronic Mail Standards |
| Subsection 5.2 | FAX Standards |
| Subsection 5.3 | Bulletin Board Standards |
| Subsection 5.4 | Electronic Data Interchange (EDI)) Standards |
| Subsection 5.5 | Voice, Video, and Image Telecommunications |

## 5.1 Electronic Mail Standards (E-Mail)

The term E-mail refers to a service that allows the transmission of electronic correspondence (messages) over a computer network. E-mail server or gateway is used to describe a network device that stores or transmits messages from one E-mail server to another. The term E-mail administrator refers to an individual responsible for the administration, operation, maintenance, and backup of an e-mail server or gateway. E-mail users are users are those who send or receive electronic correspondence (messages).

E-mail messages originated in the SDLC E-mail system are the property of SDLC. Emails originating outside of the SDLC E-mail system are the property of the originator.

This section sets the security standards for SDLC E-mail systems and correspondence using these systems.

### 5.1.1 E-mail Users

a) E-mail correspondence must have a valid business purpose as described in SOP.
b) Every E-mail user must be uniquely identified within the SDLC Enterprise by their own separate E-mail account to the host providing e-mail access.
c) Use of another associates E-mail account for any reason is prohibited, unless compensating controls are in place, and management specifically approves it.
d) Use of shared e-mail accounts must fully comply with the standards for shared system accounts as identified in section 2 of this document.
e) SDLC E-mail accounts must not be forwarded to a non-SDLC E-mail account.

#### 5.1.2 E-mail Servers and Gateways

Production E-mail servers and gateways on the SDLC computer network must comply with the same guidelines set forth in this document. In addition, the following standards apply:

a) Each production E-mail server and gateway must have a primary and secondary E-mail administrator identified, who is responsible for the account administration, maintenance, and backup of the system.
b) E-Mail gateways are generally implemented as single purpose machines and must be secured in a protected area per Section 6.

#### 5.1.3 E-mail Administrators

a) E-mail administrators must ensure that accounts are properly maintained. Procedures must be documented and in place for handling activation, de-activation, and removal of E-mail accounts.
b) E-mail accounts for individuals no longer requiring access, or no longer with SDLC must be disabled immediately and permanently removed within three months. E-mail account and E-mail core directory maintenance must comply with the general guidelines for account maintenance in Section 2.
c) Explicit management consent is required before an E-mail or system administrator may access E-mail messages that are not their own. A management approved process must be documented and must be used for those recurring situations where access may be necessary, providing the access complies with all local and regional laws.
d) E-mail administrators must ensure that all users of the systems they are responsible for are familiar with SDLC's E-Mail Appropriate Use Guidelines.
e) E-mail administrators must develop backup and disaster recovery procedures for the E-mail servers and gateways in their area of responsibility per Sections 7 and 8.

#### 5.1.4 E-Mail Enabled Applications

a) E-mail systems and messages must not be used for information that requires non-repudiation unless additional controls, e.g. digital signatures or manual confirmation procedures are added.

#### 5.1.5 POPI Classification of E-mail Messages

a) All E-mail messages classified Internal Use and above must be properly classified as part of the message body in accordance with SOP.
b) Information classified as Internal Use and above must be encrypted if sent from a system attached to a SDLC network to anyone outside of the SDLC network.
c) SDLC Registered Secret Proprietary information must be transmitted in encrypted format at all times.

**The following POPI classification matrix outlines the requirements for sending E-mail messages internally, externally, and across wireless networks.**

| POPI Classification of Information | Encryption Requirement |
|---|---|
| General Business Information | No Encryption Required |
| SDLC Internal Use Only | No Encryption Required if sent within the SDLC Network.<br><br>Encryption is required if sent across a non-SDLC Network or across a Wireless Network. |
| SDLC Confidential Proprietary | No Encryption Required if sent within the SDLC Network.<br><br>Encryption is required if sent across a non-SDLC Network or across a Wireless Network. |
| SDLC Registered Secret Proprietary | Encryption is Always required. |

## 5.2 Fax and Telex Standards

A fax machine is a device that scans pages, converts the images to digital format, and then transmits the image across telephone lines. A fax machine can send or receive data. Fax machines are electronic devices that are subject to the same standards set forth in this document for computer systems. The following additional standards apply for fax machines.

a) Only faxes pertaining to SDLC business are allowed into SDLC. Unsolicited incoming faxes offering products or services for sale are discouraged.
b) Any fax or telex transmission initiated within SDLC containing information which is classified SDLC General Business Information may be transmitted without indication of classification. If the data is classified Internal Use Only, it must specify this classification on the transmission, as required by POPI (Section 1.3.1). No data classified CCP or higher may be transmitted via telex or fax.
c) Fax machines must be turned off during non-business hours.
d) The fax feature of any machine supporting both faxes and data signals must be disabled when data transmission is active. If a fax device also supports dial-in data reception, data reception must be protected as required in section 3.2.
e) Fax cover sheets must specify that the fax is intended for exclusive use of the addressee and may contain information that is confidential, proprietary, or privileged. It must also state that if the fax communication is received in error, the recipient is strictly prohibited from any dissemination, distribution, copying, or use.

## 5.3 Bulletin Board Standards (including blogs and discussion forums)

Electronic bulletin board systems are computer-based facilities that can make information available to a world wide audience.

A bulletin board system often operates on an open, public access basis where individuals use the system without first identifying themselves. Information contained on electronic bulletin board systems is available from various sources and is offered "as is" for and by people in the user community. Placing information on a bulletin board is called "posting".

Some bulletin board systems allow information to be posted into separate "newsgroups". Public newsgroups contain information for general public discussion. SDLC-wide newsgroups contain information that can be shared anywhere within SDLC. SDLC-limited newsgroups also exist to convey information to a particular group of users.

Electronic bulletin boards must be used for necessary business purposes only.

#### 5. 3. 1 Individual Identity

a) A login id and password is required before an individual can access the articles on any SDLC newsgroup.
b) All persons posting to a SDLC bulletin board must identify themselves by name.

#### 5. 3. 2 Data Classification

a) Any general information, software fixes, public domain software or documents may be posted on an electronic bulletin board system unless prohibited by the originating author. Software must not be posted if its posting causes violation to any distribution rights.
b) Any information classified as SDLC Internal Use Only must only be posted to SDLC newsgroups, not public domain bulletin boards.
c) Any information classified higher than SDLC Internal Use Only may not be posted on any bulletin board system.
d) Information pertaining to questionable security practices or breaches must not be posted to any BBS.
e) A bulletin board is not the appropriate place for posting of sensitive personal data which intrudes on a person's privacy, for example discussion of a health problem which is making an employee absent from work.
f) News provided strictly for SDLC customers, contractors, suppliers, or business partners must only be posted on SDLC-limited newsgroups.

#### 5.3.3 Publishing Standards

a) No racially/ethically sensitive or otherwise obviously offensive information shall be posted or allowed to be posted to SDLC News groups or BBS.
b) No person shall post any information or programs that will cause a compromise to the security or integrity of a SDLC system. Such programs include, but are not limited to, viruses, worms, and Trojan horses.
c) The detection of prohibited information on an electronic bulletin board will result in immediate cancellation of the posting. The person(s) who posted the information must be identified and reported to management. Continual misuse of bulletin board privileges will be subject to disciplinary action as stated in the corporate personnel policy.

#### 5.3.4 BBS Administration

a) A system administrator must be assigned for each bulletin board service.
b) The newsgroup or BBS system administrator must define the maximum classification of information allowed by the newsgroup whenever a newsgroup is created.

## 5.4 Electronic Data Interchange (EDI) Standards

Electronic Data Interchange (EDI) is the electronic exchange of data between different companies by computer applications using agreed-upon message standards without any human intervention. Each company that sends and/or receives documents via EDI is referred to as a trading partner.

Electronic Data Interchange allows business to be conducted with paperless, electronic transactions. EDI improves process speed and accuracy while reducing the costs associated with handling paper transactions. Trading partner relations are improved because EDI encourages a large amount of cooperation and communication between companies.

SDLC's trading partners (customers, suppliers, joint ventures, etc~) translate their business application information into a mutually compatible data communication format such as ANSI X.12 (U.S.) or EDIFACT (International). The following are examples of applications using EDI services: processing purchase orders, invoices, and electronic funds transfer (e.g. payroll direct deposits, or paying bills electronically).

EDI may route information through public data networks, enterprise networks, inter-enterprise networks, value added network services or the Internet. A third party to handle common data communication and management functions for trading partners supplies VAN services. This benefits a trading partner by only having to converse with one communication system.

#### 5.4.1 EDI Data Security Software

a) Data security software must protect EDI transactions, programs, and files from unauthorized access by trading partners and SDLC employees.
b) The data security software must report authorized use of EDI transactions as well as all unauthorized attempts must produce an audit trail. The individual responsible for the EDI transfers must review the audit trail for unauthorized attempts weekly.
c) Trading partners must establish security controls to verify the authenticity of data received.
d) Trading partnership data will be assigned a security classification based on Protection of Proprietary Information (POPI Section 1.3.1) requirements regarding sensitivity of data and access authorization.
e) Trading partner data will be segregated in a manner such that a trading partner only has access to data required for its business application.
f) All passwords associated with EDI transaction processing (operating system, VAN, and application software) must minimally meet the SDLC password requirements established in the General System Integrity and Access Control Standards (Chapter 2).

#### 5.4.2 Trading Partner Accounts

a) Trading partner accounts cannot be activated until a trading partner agreement has been signed and approved.
b) The trading partner agreement must either be signed by the Sector/Group Controller or General Manager (SIC)
c) The individual who signed for the account must review trading partner accounts and data access authorizations on an annual basis.
d) Trading partner accounts must be terminated within twenty-four hours of cancellation notice by the EDI client business unit.

#### 5.4.3 Security Controls

a) Security controls must be in place for EDI data routed through public data networks, the Internet, enterprise networks, value added networks and value added network interconnections.
b) Dial up security controls for EDI systems must minimally meet the SDLC requirements defined in the Section 3.

#### 5.4.4 Auditing

a) Application error recovery procedures must exist for EDI messages in the event of processing errors.
b) An audit log of all EDI transactions must be retained as per Corporate SOP's.
c) A business resumption/disaster recovery plan must be in place for EDI transaction processing. (See Section 7.0)

## 5.5 Voice. Video and Image Telecommunications

Ongoing day to day events and experiences regarding voice security issues, along with estimates of projected losses to companies such as SDLC through fraud, abuse and compromise, have been rising at an alarming rate. It is therefore SDLC's responsibility to have the necessary tools, policies, practices and standards implemented to protect SDLC's assets and information. For the purpose of this document the following are considered as voice Application systems; PBX's (Private Branch Exchanges),Telephone systems referred to as Key Systems, Centrex service, Voice Mail, Image technology (e.g. Video), and Fax.

Voice systems technologies share many security similarities with Information Processing systems i.e. information sensitivity, passwords, direct system access and remote system access. Voice system technologies do however differ in some significant ways, which are the primary focus of this section. Information transmitted through voice technologies involve temporary, on demand, randomly scheduled, unscheduled, and dial-up connections which make security protection more difficult. These technologies communicate information of a wide-spread value and sensitivity.

The following will define major security areas of concern and identify those SDLC standards required to minimize those voice security vulnerabilities.

#### 5.5.1 Voice System Administration

The standards defined in this section pertain to PBX's, Key Systems, and Centrex Service:

a) The risk level of the information to be transmitted must be assessed according to POPI (Section 1.3.1) sensitivity classification before using voice, fax, or image technologies.
b) This assessment must be the cooperative effort of both the service provider and the user.
c) Cryptographic protection of voice communications must be used where the information exchanged is classified as SDLC Confidential Proprietary or above unless legally prohibited.
d) All system output logs and/or history files that reflect voice System activities must be reviewed on a daily basis for unusual activities or entries, i.e. invalid log on attempts.
e) All system activity printed reports such as output logs or Call detail reports must be treated as Confidential material and must be labeled, handled and disposed of in accordance with SDLC's policies and procedures.
f) All system documentation, access codes, passwords and directories must be treated as SDLC Confidential Proprietary data.
g) All unused or vacant telephone extensions must be removed from the voice system as required for account administration according to Section 2. If removal is not practical, the vacant or unused extensions must be restricted to allow only internal calling. All other calling capabilities for these extensions must be removed or denied.
h) System calling restrictions must be applied whenever possible to calling areas classified as high risk areas in all countries.
i) System calling restrictions must be applied that deny all calls to nonessential numbers such as calls to "services Billed to the calling number". Examples include 900 numbers in the United States, 0898 numbers in the United Kingdom, and 600 numbers in Asia.
j) All menu driven applications, i.e. call controllers that allow a choice of options must restrict those options to allow only internal selections. If however, external selections are a business requirement, then the external option must be specific and auditable.
k) All voice processing equipment must be located in a secured Area with limited authorized and controlled access.
l) Physical audits of all voice communications equipment, extensions, voice mail boxes, telephone lines, and services must be conducted at least once a year.
m) All administrative passwords must immediately be changed whenever system administration responsibilities change per the standards set forth in Section 2.

#### 5.5.2 Voice System Features

This section addresses security standards for specific voice system features on PBX's, Key Systems, Centrex Service:

a) System feature capabilities must only be allowed that meet the specific SDLC operational and/or facility requirements. All other system features that are not required or jeopardize SDLC's security standards must be denied, unless a risk assessment has been performed and management authorization exists.
b) Telephone station capabilities must only be allowed for individual users and departments after a requirements survey has been completed and approved that defines those specific needs and requirements.
c) All voice system and station capabilities that are not required to support SDLC's facilities, departments or individual users must be denied.

#### 5.5.3 Trunk Systems

a) All system trunking must be reviewed for compliance with the following standards on a yearly basis.

b) PBX system trunk access passwords must be a minimum of 12 characters in length and must be managed and maintained with the same confidentiality controls as related to computer System passwords.
c) Trunk to Trunk transfer must always be denied. If Trunk to Trunk transfer is a business requirement, then the liabilities and exposures for using this feature must be documented and fully understood and approved by the Sector Controller.
d) Direct Trunk Access must always be denied. Trunk access Codes must adhere to existing password controls as related to computer system passwords whenever possible.
e) With Direct Trunk Access denied, Trunk Access codes need only be changed once every 12 months.
f) Access to all external voice mail trunking must be denied. If access to external trunking is required for business purposes, a risk assessment must be performed to identify the liabilities and exposures for allowing access, the requirements documented, the connection approved by the Sector Controller and calls must only be allowed to specific auditable numbers.
g) Voice mail trunks must never be allowed to directly access an external operator or receive external dial tone.

#### 5.5.4 Call Forwarding

a) Call Forwarding must only be authorized for use in forwarding calls to telephone extensions connected and served by the same SDLC voice communications system.
b) External Call Forwarding must always be denied. If however, External Call Forwarding is a business requirement, then the external number call forwarded to must be specific, documented, approved and auditable.
c) Liabilities and exposures for using External Call Forwarding must be fully understood and approved by the Sector Controller.
d) The external call forwarded to number must not allow any additional call forwarding.
e) External Call Forwarding must never allow the caller to receive dial tone.

#### 5.5.5 Voice System Access

a) Direct Inward System Access (DISA) must always be denied. Use of calling credit cards must be considered as an alternative to using the DISA feature. If however DISA is a business requirement then use of passwords and authorizations must be applied.
b) Liabilities and exposures for using DISA must be documented and fully understood and approved by the Sector Controller.
c) Remote system access ports are considered a standard host connection and must comply with all requirements identified in section 3 including two-factor authentication.
d) Remote system access must always be denied automatically after three unsuccessful logon attempts.
e) System access codes, passwords, authorization codes and barrier codes must all be at least six (6) digits in length and must be changed according to SDLC's password standards.

#### 5.5.6 Voice Mail

a) Voice mailboxes must be automatically locked after (3) three Unsuccessful log on attempts.
b) Voice mail passwords must adhere to existing SDLC password controls as related to the computer system passwords defined in Section 4.
c) All subscriber mailboxes must be removed for the voice mail system immediately upon termination or separation from SDLC.
d) The voice systems administrator must perform a physical audit twice a year to verify and validate the number of valid subscribers. Any invalid mailboxes must be deleted immediately.
e) Saved messages must be retained for no longer than 30 days. An administrative procedure must be in place to automatically purge saved messages greater than 30 days.

#### 5.5.7 Voice Processing and Multimedia Systems

a) The encryption feature (DES) on video conferencing equipment must be used if the topic of discussion or the information displayed is classified as SDLC Confidential Proprietary or SDLC Registered Secret Proprietary and usage complies with the local/country/regional import/export legislation.
b) Careful review of communication security needs must be made prior to using public videoconference rooms. The encryption feature must always be requested on the video conferencing equipment when information to be discussed or displayed during a domestic videoconference is SDLC Confidential Proprietary or higher. International public meeting room videoconferences mayor may not have the capability to encrypt. I f encryption is not available, the information to be presented or displayed may require modification to protect SDLC from the threat of industrial espionage.
c) The DES encryption feature needs to be ordered for export when ordering a videoconference system. The equipment supplier must handle the paperwork required by the United States Federal government to export.
d) Audio visual data relating to individuals is covered by data protection legislation in some countries. Therefore, individuals may exercise their rights, e.g. to access, the same as if data about them is held in written or computer readable form.

## 5.6 Web Publishing and Electronic Information Sharing

Today, more than ever, sensitive information is moving from paper to electronic media, such as internal and external web servers, shared files/databases, E-mail attachments, and removable media. The POPI principles apply to electronic information of all sorts, including Web pages.

The same SDLC POPI requirements that apply to printed communications apply to electronic communications. Failure to properly control information can result in substantial loss to the company, disciplinary action, and potentially exposing individuals to criminal and civil penalties. The following standards must be followed when sharing electronic information in any format.

Every SDLC employee is responsible for protecting sensitive online information, including personal information and other sensitive non-SDLC information that is under SDLC's control. Accessing sensitive online information requires explicit authorization, enforced by computer controls as identified in Sections 1.0 and 2.0.

a) All files, web pages and removable media must be labeled with the correct POPI classification. Online access controls for shared servers (web, Notes, FTP) must be implemented as follows:

| Data Classification | On-line Access Controls |
|---|---|
| SDLC General Business Information | • Files need not be labeled.<br>• Information may be shared freely subject to other non-POPI restrictions (e.g. Advertising guidelines).<br>• Appropriate controls must prevent unauthorized modification.<br>• This information is appropriate for internal and external web servers, anonymous FTP and newsgroups. |
| SDLC Internal Use Only | • Information is shared with those having a "need to know" such as the company phone directory and training materials.<br>• Classification must be displayed when viewed online, and embedded in the file where possible.<br>• On servers within the SDLC network, a password is not required for read access, since each SDLC or approved non-SDLC staff member has already used a password to gain access.<br>• On servers outside the SDLC data network, a second password or stronger authentication mechanism is required. |
| SDLC Confidential Proprietary | • Highly confidential information such as staff performance appraisals, marketing strategies and pricing data falls into this category.<br>• Classification must be displayed when viewed online, and embedded in the file where possible. On servers within the SDLC data network, a unique login ID and password is needed for each person being granted access. Each person must be authorized by the data center.<br>• On servers outside the SDLC network, strong authentication and encryption is required. |
| SDLC Registered Secret Proprietary | • MUST NOT reside on shared computer network. |

b) Compliance to all export controls and customs laws must be in accordance with the local country laws. These laws apply to the transfer of software and technical information regardless of how the transfer takes place or the fact that the recipient is another member of the SDLC staff.

c) Technical information that is being shared is subject to any local laws before it is transmitted or placed it on a server that is accessible to SDLC Staff outside the country where the server resides. For assistance in this area, contact the appropriate Sector/group export control staff for guidance in this area.

d) Approval from the local marketing department, or Corporate Communications must be given before publishing information externally, including by E-mail. This ensures compliance with legal requirements and regulations, SDLC's branding and style guidelines, and local cultural/advertising etiquette. Management must approve any statements which could be perceived as official SDLC positions or endorsements.

e) Compliance must be met regarding licensing agreements and other applicable intellectual property, trademark, copyright, and contract requirements.

# 6.0 PHYSICAL AND ENVIRONMENTAL SECURITY STANDARDS

**Purpose:**

To define the physical security standards which support the SDLC Corporate Security Policy and Procedure Manual for protection of computer and information assets (data).

**Background:**

Even though today's computing environment has moved from large computer centers to distributed, portable, mobile and desktop machines, the need to ensure physical security and environmental standards are maintained is crucial. Critical or sensitive computing applications must be contained within a secure, controlled and monitored environment to prevent unauthorized access or damage. However, physical security must be consistent with the value of the asset to be protected.

The basis for this section is to supplement the standards already defined in the SDLC Standards of Internal Control.

**Scope:**

These standards apply to all computer hardware platforms used in the execution of SDLC business. Examples include, but are not limited to all computers used in manufacturing, engineering, office and home environments.

These standards apply to all SDLC computers, and any outsourced computer environments. SDLC does not permit under any circumstances, the use of privately owned computer hardware and/or software for company business.

Physical security is essential to securing information; without it, information is open to easy creation, modification, interception and destruction via physical access or physical hazards. Site location, construction, fire and flood protection, environmental safeguards and physical access controls are key elements of a physical security program. Physical security controls and a physically secure area are already explained and described in the SDLC Corporate Security Policy and Procedure manual, available from your local physical security manager. The following standards support that document.

Section 6.0 includes the following subsections:

| | |
|---|---|
| Subsection 6.1 | File Servers, Telecommunications Equipment |
| Subsection 6.2 | Computer Workstations |
| Subsection 6.3 | Printer/Fax Physical Security |
| Subsection 6.4 | Environmental and Hazard Protection |
| Subsection 6.5 | Hardware Security and Maintenance |

## 6.1 Physical Access Controls and Monitoring of Secure Computing Areas

Physical access controls restrict access to only authorized personnel and are applicable to SDLC secure areas and any outsourced computer operation.

### 6.1.1 Computer Centers

a) Computer centers must be located in a secure environment with access restricted to authorized personnel only.
b) A list of authorized personnel must be documented and reviewed at a minimum annually to ensure that access is still required. Unauthorized personnel (e.g. visitors, maintenance support personnel) must be escorted at all times.
c) Detailed logs must be kept of all persons entering a secured environment.
d) All entrances must be physically secured (SIC) with card access controls or equivalent security in place.
e) Video monitoring equipment must be installed to monitor particularly sensitive locations

## 6.2 Telecommunications Equipment

This section defines the physical security standards for telecommunications equipment (e.g. routers, dataline termination boxes, patch panels, etc.)

a) Telecommunications equipment must be located in a physically secure and locked environment. For example, a router can be placed in a wiring closet or open office, but physical access must be restricted to the unit by being placed in a locked key cabinet or closet. There must be restricted logged access for the keys and a record or authorized personnel gaining access must be maintained.

## 6.3 Computer Systems

Physical security controls for computer systems protect the equipment and the stored data from damage and loss. Physical security is the responsibility of the person using the equipment and that person's supervisor as well as the facility's physical security and/or maintenance personnel. This section defines physical security standards for all computer systems.

a) The computer system must reside in a physically secure building, floor, or room. If the workstation processor is in a public or non-SDLC controlled area, it must be physically secured to prevent theft.
b) Data owners and custodians must jointly perform a risk analysis for all computer systems running shared applications, to determine when the system must be located in a computer center. All shared systems must be located in computer centers when the potential loss of information outweighs the cost of physically securing the equipment as such.
c) When physical locks are an internal part of the equipment, they must be used in addition to other forms of security.
d) Laptop or palmtop workstations must be physically locked in a desk or cabinet when unattended for overnight periods or longer. This is mandatory for all areas including open, fixed wall or lockable offices
e) Workstation equipment may only be moved after taking proper precautions against damaging the machine.

#### 6.3.1 Computer Media Handling

Media containing information must be physically treated and handled with care to maximize the reliability and integrity of the information.

a) Computer storage media must not be stapled, bound with a rubber band, or paper clipped to other materials.
b) All diskettes, tapes, or other storage media must be stored in a holder specifically designed for that purpose. Care must be taken when handling the exposed portion of storage media to minimize fingerprints on recorded surfaces.
c) Individuals using removable storage media must protect them from hazardous environmental and magnetic influences. For example, since the standard telephone on a desk contains magnets, storage media must not be placed under the telephone.
d) The individual using storage media must protect them from pressure caused by other objects.

## 6.4 Printer/Fax Physical Security

a) Printers and fax machines used to print information classified as SDLC Confidential Proprietary or higher must be located in a physically secure area, or the recipient must attend the printer/fax machine during output.
b) Recipients of SDLC Confidential or SDLC Registered Secret Proprietary information must be present at the printer or fax machine during receipt/transmission. It is the responsibility of the sender to ensure the recipient is present at the machine when receiving/printing. The transmission must not commence until the recipient has been contacted.

## 6.5 Environmental and Hazard Protection

Environmental hazards pose one of the biggest risks to workstations. Temperature extremes caused by excessive heat or sunlight can be prevented with adequate ventilation and temperature conditions. Smoking, drinking, and eating in the immediate areas of computers is restricted and must be enforced relative to the system’s criticality to the company’s uninterruptible functions. Care needs to be taken when cleaning or using solvents on or around computer equipment to eliminate environmental contaminants. Static electricity and other electrical or magnetic influences in the immediate area of the workstation present hazards that can destroy data. Radios or computer equipment may cause interference. A magnetic paper clip stand may cause disturbance. "Brown out" can cause destruction of data that might not be recognized for months after the damage has occurred.

The most common causes of equipment failure include power outages, improper heating, cooling or ventilation operation and excessive dust. The wrong amount of humidity can create a problem. Too little humidity causes static electricity while too much humidity can result in equipment corrosion.

This section describes the standards that apply to hazard protection and hardware and security maintenance.

**6.5.1 Hazard Protection**

Controls are necessary to minimize damage from natural hazards such as fire or excess water. For example, flooding can result from breaks in the cooling system or water drainage pipes. Computer equipment must be protected against natural disasters such as fire damage, water damage, or electrical surges (SIC).

a) Computer equipment must not be located near any combustible or hazardous areas (SIC)
b) Smoke detectors and fire extinguishers must be inspected/tested at least every six months.
c) Clean power is essential. Power surges can destroy data, programs, and equipment. In-Line surge protection/management devices must be used to protect against power fluctuations.
d) The power controls for electrical computer equipment, computer ventilation system(s), and computer center lighting must be maintained on isolated electrical circuits.
e) Air conditioning must be installed and maintained to prevent equipment damage caused from overheating.
f) Installation and maintenance of computer equipment must be in compliance with the environmental requirements described by the equipment supplier. Equipment must be cleaned and maintained as recommended by the supplier.
g) Information must be protected against modification by environmental hazards, line noise, and other accidents that could cause data integrity problems.
h) Care must be taken to keep electronic storage media away from environmental or magnetic influences.

# 7.0 INFORMATION BACKUP AND RECOVERY STANDARDS

**Purpose**

To state the SDLC Information Backup/Recovery standards for the protection of computer based information.

The information contained in this section is intended to supplement the standards already specified in the SDLC Standards of Internal Control.

SDLC's essential business functions are highly dependent on our computerized systems. The backup and safe storage of information is fundamental to the reliability and recoverability of each system and its supported businesses. In the event of information corruption or loss, disk hardware failure or site disaster, the backup information is often **our only link to recovery.**

**Responsibilities**

Per SIC, Information Backup and Recovery is a joint responsibility, which is shared between "the custodians of the computer applications, equipment and facilities in coordination with the application system owners." Custodians are identified as the ones who are "responsible for the operation and maintenance of the data processing equipment." Systems owners are identified as the "user or group of users with the primary responsibility for updating the application files."

Per SOP which "applies to all employees using any computer resources of SDLC or its subsidiaries worldwide" Section 2 states "Information which is critical to business operation (including data, programs, system software, and system configurations) must be backed-up periodically to ensure continuity of business operations.

These Information Backup/Recovery standards define requirements that must assist in providing for a timely recovery of SDLC's critical business activities when an outage or a disaster occurs.

Section 7.0, entitled Information Backup and Recovery Standards, includes the following subsections:

| | |
|---|---|
| Subsection 7.1 | Identifying Critical Information |
| Subsection 7.2 | Backup Requirements for Critical Business Applications |
| Subsection 7.3 | Backup Requirements for Non-Critical Business Applications |
| Subsection 7.4 | Backup Procedures |
| Subsection 7.5 | Off-Site Storage |

## 7.1 Identifying Critical Information

The degree and scope of data recovery and backup planning is driven by the potential company and business impact that would result from the loss of a particular application, data, system, and/or network.

An application's business criticality is based on several evaluation areas.

- Customer visibility measures the impact that the loss of the application would have from the perspective of SDLC customers (e.g. loss of customer or employee good will).
- Financial impact evaluates the application's business importance in terms of how its loss would effect revenue or our inability to meet financial obligations.
- The legal impact rates the application's business importance in terms of legal, contractual, governmental, or regulatory requirements.
- The impact to the corporate image that would result from the loss of an application and/or its data is also evaluated. Such a loss could seriously erode our corporate reputation and shareholder confidence. A major loss could cause an inability to function as a company or sector/group.

The methodology used to determine the criticality of business applications, data, systems, and/or networks is the Business Impact Assessment (BIA) process. The BIA process is the most important step in both backup strategies and disaster recovery planning. In this phase, a business assessment is performed on all applications and data running on the system or network being analyzed. The result of this assessment determines the criticality of the application and data to the business and to SDLC as a whole. The criticality dictates how quickly the application, data, systems and/or networks need to be recovered. This speed of recovery is then used to help design the proper recovery strategy. The BIA process also identifies how current the recovered information will need to be in order to return the business to an operational status.

It is through this process that the business recovery requirements are defined. These requirements then provide the design objectives for the Information Backup Plan, recovery plan, as well as the recovery time frame by which the effectiveness of the disaster recovery process will be measured.

The SDLC requirements for information backup has been divided into the following two recovery groups based on business defined application criticality.

- Critical Business Applications, data, systems, and/or networks are those assets where the owner has determined is essential in order for the Sector or Group to meet its customer and/or business commitments.
- Non-critical Business Application, data, systems, and/or networks are those assets where the owner has determined has a lesser business impact and can tolerate greater loss of data or longer recovery time in the event of a disaster.

## 7.2 Backup Requirements for Critical Business Applications

Because of the need for rapid recovery, often with little or no loss of data (as defined by the Business Impact Assessment process), the backup methodology, frequency and off-site storage process used for **essential** business applications may vary widely. Daily or more frequent backups, electronic vaulting, remote file mirroring, data journaling and standby processing must all be considered based on business need.

a) A Business Impact Assessment (BIA) must be performed for each business application, system, and/or network in order to establish the true level of information criticality. The criticality classification and the backup process must be reviewed/updated by the application owner and equipment custodians.

   - When the application changes.
   - When significant changes in exposure occur.
   - Minimum annually.

b) The level of information criticality must be reviewed, documented and agreed upon by the affected application owners and equipment custodians per SIC.
c) An Information Backup Plan must be developed to fully support the operating systems, software applications and data to the agreed upon level of criticality.
d) An Information Backup Plan must contain the name of the system and or data, frequency and type of backup, offsite vaulting cycle and any trade off rational used in developing the backup plan.
e) The Backup Plan must insure that in the event of a disaster, the backup information, which is stored off-site, is complete and sufficiently current so that the amount of data loss, if any, is acceptable to business management.
f) Based on the Backup Plan, information must be backed up on a scheduled basis and must, along with its documentation, be taken off-site frequently enough to insure that in the event of a disaster, the recovered data is current enough to support the business.

## 7.3 Backup Requirements for Non-Critical Business Applications

Non-critical business applications and data must be fully backed up weekly. Incremental or differential backups must be done as required by the business. Backup information must be kept physically separated from their systems, with at least one full set of backups, and associated documentation stored off site for disaster recovery purposes.

a) System, file server software, application programs and data must have full backups taken weekly.
b) The backups must be kept in an area physically separate from the systems/server(s).
c) All backup information must be stored with its documentation in a secure location.
d) Incremental or differential backups must be done based on business need.
e) A backup copy of the system, file server software, application programs, data, documentation, and other Disaster Recovery records must be kept in an off-site location.
f) Where possible, LAN/System Administrators must accomplish backups of critical local workstation information. If not feasible, users must be directed and trained to backup their own critical information.
g) Users of portable and/or remote systems are responsible for backing up and storing their data in a safe, secure location. The extent and frequency of the backup process is based on the business impact that would result from its loss. All EISS standards apply to portable and remote systems.

## 7.4 Backup Procedures

Our backup information provides protection from almost any threat -accidental or deliberate, that could cause loss or destruction of data. Below are the required backup standards for SDLC systems.

a) A documented backup process must exist which defines the daily backup routines. At a minimum, it must include the following about the backup cycles:

- System Names or functional names included as part of any backup
- Elements of the system that are backed up. This can include system names, partition names, disk names, directories, type of data, or whichever descriptive manner is appropriate for the system being backed up.
- Determination on the number of generations used

b) A locally stored backup log must be kept which at a minimum logs the following information:

- Name of media used
- Type of Backup (e.g. full backup/incremental, differential, etc.)
- Date the backup was performed
- Verification status (completed/failed)
- Any restart procedures that were required.
- Location where the backup media is stored, date it was place there, and who placed it there

c) Backup techniques used must be capable of fully restoring all open/active files so that the integrity of these files is not compromised and that they can be fully restored to active operations.
d) In distributed database environments, the backup system must ensure the synchronization of the recovery.
e) All backup media must be labeled with the highest classification of the data that resides on the media.
f) All locally stored backup media must be kept in fire retardant media safes. Access must be limited to those who perform the backups. A log of the media in the safe must be maintained for use as a recovery aid.
g) Backup procedures must exist for handling daily backups as well as performing day-to-day restorations or full data recovery.
h) The backup process must be automated wherever possible in order to ensure consistency.
i) Randomly selected file restores must be performed at a minimum of monthly to ensure the readability of the backups (i.e. data is actually being written to tape) and to ensure that tape media is still readable.
j) Wherever feasible, backups must be verified by reading them back after they are written. Many backup software packages allow this to happen in conjunction with routine scheduled backups.
k) Backup media devices must be periodically cleaned per manufacturers specifications to ensure the integrity of data being written to them.

## 7.5 Off-Site Storage

Off-site information storage is defined as a secure off-campus location that is sufficiently distant from the primary location so that, in the event of a localized or area wide disaster, the backed up information will be safe and available for recovery. This could be a remote mainframe system or server available via the SDLC peer-to-peer network, another SDLC site, or an off site storage facility. The following Standards apply to all off-site storage locations.

a) The off-site location must have restricted access, yet be accessible when needed, at any time, night or day. If an outside company operates the location, it must be bonded and insured against loss or breach of security.
b) Off-site backup media must be given the same level of physical and environmental protection that are required for the primary site as defined in Sections 1,2,4,6 and 7 of this document. This includes security during the transporting of media and documentation between SDLC and the off-site location.
c) A documented procedure must be in place that outlines the off-site rotation process. At a minimum this must include a list of who is authorized to send data off-site, who is authorized to recall data, and who is authorized to make changes in access levels of SDLC employees.
d) A process must be in place for reviewing who has access to off-site processes. This review must be done at a minimum annually -or whenever there is a change in responsibilities that warrants it.
e) When off-site data is kept for multiple years, the media must be brought back and tested for integrity at a minimum annually. Data should be copied to new tapes at a frequency level that ensures data will not be lost per specifications of the type of media used. This must be performed more frequently when off-site data is extremely sensitive and is being kept for archival or legal purposes.

# 8.0 DISASTER RECOVERY PLANNING STANDARDS

**Purpose**

To state the SDLC Disaster Recovery Planning standards and responsibilities which are required for the protection of all business critical hardware, systems, applications and networks.

**Scope**

The information contained in this section is intended to supplement the standards already specified in the SDLC Standards of Internal Control.

SDLC's essential business functions are highly dependent upon our computerized information systems. Natural (e.g. floods, storms, earthquakes) or man-made (e.g. sabotage, operator error, equipment failures) disasters can terminate or severely disrupt business-processing capabilities. Disaster Recovery Planning provides for the timely resumption of SDLC's essential business hardware, systems, applications and networks in the event of a disaster.

**Responsibilities**

Per SIC sections 8, Disaster Recovery Planning is a joint responsibility which is shared between "the custodians of the computer applications, equipment and facilities in coordination with the application system owners." Custodians are identified as the ones who are "responsible for the operation and maintenance of the data processing equipment." Systems owners are identified as the "user or group of users with the primary responsibility for updating the application files."

Because of this shared responsibility, someone must be selected to function as the Disaster Recovery Planning Coordinator. The Disaster Recovery Planning Coordinator will then work with the various areas in the development, testing and updating (maintaining) of the plan.

Section 8.0, entitled Disaster Recovery Planning Standards, includes the following subsections:

| | |
|---|---|
| Subsection 8.1 | Identifying Critical Applications |
| Subsection 8.2 | Developing the Disaster Recovery Plan |
| Subsection 8.3 | Testing the Disaster Recovery Plan |
| Subsection 8.4 | Training |

## 8.1 Identifying Critical Applications

The degree and scope of the Disaster Recovery Planning process is totally driven by the potential company and business impact that would result from the loss of a particular application, hardware, system, network and/or data.

An application's business criticality is based on several evaluation areas.

- Customer visibility measures the impact that the loss of the application would have from the perspective of SDLC customers (e.g. loss of customer or employee good will).
- Financial impact evaluates the application's business importance in terms of how its loss would cause a loss of revenue, impact time to market or our inability to meet financial obligations.
- The legal impact rates the application's business importance in terms of legal, contractual, governmental, or regulatory requirements.
- The impact to the corporate image, which would result from the loss of an application and/or its data, is also evaluated. Such a loss could seriously erode our corporate reputation and shareholder confidence. A major loss could cause an inability to function as a company or sector/group.

The methodology used to determine the criticality of business applications, systems, networks and/or data is the Business Impact Assessment (BIA) process. The BIA process is the most important step in Disaster Recovery Planning. In this phase, a business assessment is performed on each application running on the system or network being analyzed. The result of this assessment determines the criticality of the application to the business and to SDLC as a whole. The criticality dictates how quickly the application needs to be recovered. This speed of recovery is then used to help design the proper recovery strategy. The BIA process also identifies how current the recovered data will need to be in order to return the business to an operational status.

It is through this process that the business recovery requirements are defined. These requirements then provide the design objectives for the data backup plan, recovery plan as well as the recovery time frame by which the effectiveness of the disaster recovery process will be measured.

The section identifies the criteria for determining critical business applications.

a) A Business Impact Assessment (BIA) must be performed for each business application, data, system and/or network in order to establish the true level of business and data criticality.
b) The recovery timeframe must be reviewed, agreed upon by the affected business and Information Systems areas (system / data owners and equipment custodians per SIC) and documented.
c) The criticality classification must be reviewed/updated by the system owner and equipment custodians:
    - When the application changes,
    - When significant changes in exposure occur, or at a minimum,
    - Annually.

Once the Business Impact has been determined, a Site-Risk Assessment must be performed to identify problems before they occur.

## 8.2 Developing a Disaster Recovery Plan

A Disaster Recovery Plan must contain all of the detailed steps, procedures and support information needed to recover the subject hardware, system, application and network in the event of a disaster.

This section describes the standards for developing a disaster recovery plan:

a) A Disaster Recovery Coordinator must be assigned to coordinate the development, testing and updating (maintaining) of the plan.
b) Each system owner / equipment custodian must develop and document a Disaster Recovery Plan for each essential business application, system and/or network it supports.
c) Because of the sensitive nature of the material contained in the recovery plan, it must be classified as SDLC Confidential Proprietary.
d) Information Security procedures and mechanisms must be maintained during the recovery process.
e) Each Disaster Recovery Plan must be reviewed using the Disaster Recovery Plan Review Check List.
f) The plan must be tested and updated yearly to reflect changes in the hardware, system, network and/or application.
g) A copy of the recovery plan, documentation and supplies must be kept in a secured off-site location.

## 8.3 Testing the Disaster Recovery Plan

It is impossible to overstate the importance and value received from testing the disaster recovery and back-up plan. Only through testing will any missing and/or critical pieces be identified that could have rendered the system UNRECOVERABLE. This section identifies the standards for testing a disaster recovery plan.

a) System owners and equipment custodians are responsible for testing their Disaster Recovery Plans at least once a year to ensure that the plans are accurate, complete and that the off-site data can be used to successfully recover the application. Where testing of the full plan is impractical, individual sections or sub-systems must be tested separately in order to confirm the recoverability of the plan as a whole.
b) The test recovery must be successfully completed with the hardware, system, network, application programs, data recovered and the applications functionally verified by the business or application support areas within the recovery time frame that was defined in the Business Impact Assessment process. Failed tests must be re-tested, within a timeframe that is agreeable to the business area, until completed successfully.
c) More frequent testing must be considered when a system, application and/or network has experienced a high degree of change.
d) When performing the test, all materials, i.e. procedures, data, documentation, etc. needed to facilitate the recovery test must come from locations other than the primary processing site.
e) Where possible, personnel who are unfamiliar with the site being tested must be used to execute the recovery test in order to verify the detail and completeness of the recovery procedures.
f) A sequential log of test events must be kept which lists time frames, problems encountered and suggestions for improvement. This log must be expanded in a postmortem review and then used for problem tracking and resolution. The full test must be reviewed with the supported business(s).

## 8.4 Training

a) All Disaster Recovery Coordinators must attend the Disaster Recovery Planning Workshop class that is offered by SDLC University. The appendix contains information on the two MU Disaster Recovery Planning classes.

# APPENDIX A – LIST OF ACRONYMS

| Acronym | Description |
|---|---|
| ACL | Access Control List |
| BBS | Bulleting Board System or Blog Board System |
| BIA | Business Impact Analysis |
| CCDS | SDLC Communications Distribution Systems |
| CCERT | SDLC Computer Emergency Response Team |
| CCP | SDLC Confidential Proprietary |
| CDNA | SDLC Data Network Architecture |
| CIUO | SDLC Internal Use Only |
| CNIC | SDLC Network Information Center |
| CRSP | SDLC Registered Secret Proprietary |
| DID | Direct Inward Dial |
| DISA | Direct Inward System Access |
| DMZ | Demilitarized Zone |
| EDI | Electronic Data Interchange |
| EISS | Electronic Information Security Standards |
| ESM | Enterprise Security Manager |
| FBN | Facility Backbone Network |
| GBI | General Business Information |
| HTTP | Hyper Text Transfer Protocol |
| LAN | Local Area Network |
| NIA | Network Interconnection Architecture |
| PBX | Private Branch Exchanges |
| PDA | Personal Digital Assistant |
| PIN | Personal Identification Number |
| POPI | Protection Of Proprietary Information |
| PtP | Peer-to-Peer |
| ROM | Read-Only Memory |
| SIC | Standards of Internal Control |
| SNA | Systems Network Architecture |
| SNIC | Sector Network Information Center |
| SOP | Standard Operating Procedure |
| SSL | Secure Socket Layer |
| TSR | Terminate and Stay Resident |
| VAN | Value Added Network |
| VxD | Virtual Device Driver |
| WAN | Wide Area network |
| WWCP | Worldwide Corporate Financial Policy |

# APPENDIX B – GLOSSARY OF TERMS

This glossary defines the terms and language conventions used throughout this manual in order to help the user in fully understanding its content.

Terms are presented in alphabetical order for easy reference.

| Term | Definition |
|---|---|
| **Access** | The ability and the means necessary, to store or retrieve data, to communicate with, or to make use of any resource of a data processing or telecommunications system. Gaining entry, physically or electronically, to a computer facility, system, or data. |
| **Access Control** | A means of limiting access to system resources. |
| **Access Control List** | One or more specific "rules" which enables specific access to or processing of information routers, gateways, and intelligent switches to define acceptable network access connections. Also used to assign access rights to specific users in certain hosts. |
| **Access Control Mechanisms** | The hardware, software, or firmware features in combination with operation and management procedures designed to detect attempted access, permit authorized access, and prevent unauthorized access to a computer system or any resource on the system. |
| **Accountability** | The quality or state that enables a security system to trace activities to the individuals who may be held responsible. |
| **ACL** | Acronym for Access Control List. (See Access Control List for definition) |
| **Approved** | May have various meanings in different contexts. For questions about the approval for your specific situation, contact your Information Security Council representative. |
| **Asymmetric Key Encryption** | A two key method of maintaining encryption keys. One (often public) key is used to encrypt information; a second key (always private) is used to decrypt the same information. |
| **Audit Trail** | A record of system activities that, when reviewed, provide enough information about the events that the time, place, subject and object can be identified. |
| **Authentication** | The act of verifying the identity of a subject. |
| **Backup** | The process of copying critical data and software for the purpose of recovering essential processing back to the time the backup was taken. |
| **Bulletin Board System (BBS)** | Generally, a public access facility making information available on an "as is" basis for and by the user community. Information contained on a BBS is accessed by related topics into newsgroups. |
| **Business Application System** | A collection of individual computer applications and data used to accomplish a given business process. |
| **Business Impact Assessment** | The methodology used to determine the impact to the business resulting from the loss of critical applications, data, systems, and/or networks. |
| **Business Unit** | An organizational entity. May be a SDLC sector, group, division, department or a joint. Venture |
| **Computer Center** | A mainframe or mini computer data center. |
| **Computer Security** | Encompasses all procedural and technical measures required to:<br>• Prevent unauthorized access to and modification, use, and dissemination of data stored or processed by a computer system.<br>• Prevent any deliberate denial of system service.<br>• Protect the system from physical harm and theft. |
| **Computer System** | In a general sense, any desktop or portable computer. In this case a computer system can be a UNIX engineering workstation (e.g. HP, SGI, Sun), a DOS-based personal computer (PC), and NT System, or a Macintosh PC. This definition would also include laptop and even palmtop computers. In more limited contexts, computer system refers to engineering computers, usually more powerful than large-scale PC's, and usually UNIX-based. For the purpose of these standards, a computer system encompasses all of the above types of intelligent computers. |
| **Confidentiality** | The requirement to protect sensitive information from disclosure to unauthorized persons. |
| **Contingency Plans** | The establishment of emergency response, backup operation, and post-disaster recovery processes maintained by an information processing facility or for an information system.<br><br>Contingency plans establish the strategy for recovering from unplanned disruption of information processing operations. The strategy includes the identification of what must be done, who performs the required action, and what tools must be used. |
| **Critical Information** | Data determined by the data owner as mission critical or essential to business purposes. |
| **Cryptographic** | Providing a means of encryption using one of the three methods, one-way, symmetric or asymmetric. |
| **Custodian** | Custodians of information assets are personnel who support and maintain information systems, computers, and telecommunications equipment. They provide physical asset control suitable to the classification of data under their custody to ensure the confidentiality, integrity and availability of information |

| Term | Definition |
|---|---|
| **Data Integrity** | The assurance that information is the same as its originating source form; i.e.: assuring that information has not been exposed to accidental or malicious modification, alteration, or destruction. |
| **Data Journaling** | The process of transmitting transaction level data to a remote location so that in the event of a disaster, restoration can be accomplished with a minimum amount of lost data |
| **Data Security** | The practice of protecting data from accidental or malicious modification, destruction, denial of service or disclosure. |
| **Digital Signature** | The result of using an asymmetrical cryptographic process to validate that a given electronic document was created only by a designated originator, and was not altered in any way prior to its receipt. |
| **Electronic Data Interchange (EDI)** | The electronic exchange of business data between different companies by computer applications using agreed-upon message standards. EDI does not involve any human intervention. EDI may route information through public data networks, enterprise networks, inter-enterprise networks, or value added network services |
| **Electronic Mail (E-Mail)** | Formal or informal communications electronically transmitted or delivered. |
| **Enterprise Networks** | See Intra-enterprise Networks. |
| **External Network Services LAN** | A SDLC LAN used to interface with non-SDLC networks. Also referred to as a demilitarized zone (DMZ). |
| **External Networks** | An external network is made up of non-SDLC nodes. |
| **Facility Backbone Network (Tier II)** | An electronic information transport mechanism carrying voice, image, and data traffic within the confines of a single facility or campus |
| **File Server** | A network component dedicated to serving and/or storing data. |
| **Firewall** | One of several types of intelligent devices (such as routers or gateways) used to isolate networks. Firewalls make it difficult for attackers to jump from network to network. A double firewall is two firewalls connected together. Double firewalls are used to minimize risk if one firewall is compromised. |
| **Freeware** | Software provided by vendors at no charge. Freeware developers often retain all rights to their software, thus preventing users from copying it or distributing it further. |
| **Gateway** | Hardware or software that is used to translate protocols between two or more systems. |
| **Guideline** | A suggested but non-compulsory approach that supports the objective of a standard. |
| **Host** | An intelligent device which stores or processes information in various forms, which must be configured or managed, regardless of whether an end-user interacts directly with the device.<br><br>Examples include:<br>• Computers (mainframe, personal, mini)<br>• Connection devices (router, gateway, concentrator, encryptor)<br>• Image processors (facsimile, video conference)<br>• Messaging systems (E-mail, voice mail, pager terminal)<br>• Telephone equipment (PBX, modem, smart or secure phone) |
| **Information Assets** | Any major assets associated with an entire information system, such as software and data. Information assets include databases, data files, application systems, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements, application systems and other collections of data. |
| **Integrity** | See Data Integrity. |
| **Inter-enterprise Networks** | Inter-enterprise networks provide connections that enable users from different companies to communicate electronically. |
| **Internal Network** | An internal network is made up of nodes which are all operated by SDLC. |
| **Intra-enterprise Networks (Intranets)** | Intra-enterprise networks only transmit communication within a single company. |
| **Local Area Network (LAN Tier III)** | A geographically small network of hosts and supporting components used by a group or department to share related software and hardware resources. |
| **Mainframe Computer** | A large scale computer with processing capability to support large scale calculations and large numbers of users |
| **Media Safe** | A safe that stores electronic media, which does not allow its contents to exceed 125 degrees Fahrenheit. |
| **Modem** | A device that supports a telephone connection between computers. |
| **Netnews** | Refers to the software used on many computer systems to allow access for posting and reading information on the Usenet electronic bulletin board. |
| **Network** | An arrangement of computers and peripherals (e.g. printers) linked by communications facilities; an arrangement of nodes and connecting cables. |
| **Node** | In a network, a point at which one or more functional units connect hosts or other networks. |
| **Non-repudiation** | A condition in which the sender cannot deny sending information and the receiver cannot deny receiving information. |
| **Object** | In relation to security events, the system (CPU), data, or other resource where access is attempted by a subject (e.g. person, terminal). |

| Term | Definition |
|---|---|
| **Off-Site** | A secure offcampus location that is sufficiently distant from the primary location so that, in the event of a localized or area wide disaster, the backed up information will be safe and available for recovery. A storage area for backed-up information which is not subject to the same risks as the location where the information originated from. |
| **One-way Encryption Key** | A one key method where the key is applied to some information and the information can never be decrypted. Also known as a hash key. |
| **Owner** | The organization or person(s) who financially owns computer hardware, software or data. They typically have overall responsibility for the hardware, software or data, it's classification, and control of whom has access to it. |
| **Peer-to-Peer Network** | A collection of nodes that reside in the same network layer. The SDLC Intranet. |
| **Penetration Testing** | A protocol followed which seeks to uncover system and network vulnerabilities. |
| **Physical Security** | Guards, badges, locks, alarm systems, and other measures to control access to computer equipment. |
| **Policy** | A brief document that announces the high level corporate position, states the scope of the policy, and establishes the responsibilities for implementation. |
| **POPI Classification** | The sensitivity of information as defined in SOP. SDLC classifications are<br>• General Business Information (GBI)<br>• SDLC Internal Use Only (IIUO)<br>• SDLC Confidential Proprietary (ICP)<br>• SDLC Registered Secret Proprietary (IRSP) |
| **Privileged Access** | Access to system and security level controls. Access rights that supersede permissions on objects. |
| **Procedure** | A set of steps performed to ensure that a standard is met. |
| **Production** | Computer systems/programs relied on by management for conducting, recording, or reporting business operations. |
| **Proxy** | A term used to refer to a network component that substitutes the true source of a network packet. This allows Internet communication without revealing network addresses. |
| **Public Data Network** | Public data networks, such as the Internet, are open to public access from anyone around the world. |
| **Public Domain Software** | Software acquired, often without charge, when the source takes no responsibility for the integrity or maintenance of the software. Note: software written by a SDLC employee or agent belongs to SDLC and must not be distributed as public domain software However in some cases, (e.g. Open Software Foundation Software license) any changes made by SDLC must be made publicly available. |
| **Reverse Proxy** | A proxy used to establish a connection between a requestor or an external user and an internal service. |
| **Router** | A network component which transfers traffic from one network segment to another based on established rules. |
| **Screen Blanking Technique** | A mechanism which darkens or obscures a display, and locks the keyboard and mouse must automatically activates after a period of no user activity, and requires authentication to regain access. |
| **Security** | Prevention of the unauthorized disclosure, corruption, modification, loss, or creation of information, as well as prevention of denial of access to information or services by authorized users. Security is a responsibility we all share. |
| **Sensitive Information** | Information that can result in loss to the corporation if it is accessed by or disclosed to unauthorized parties, or if it is fraudulently modified or updated. |
| **Shareware** | Software where the license permits free sharing and copying, but where the author retains the copyrights. |
| **Standard** | A mandatory company or divisional rule that measures compliance to policy, |
| **Subject** | In relation to security events, the person, terminal, location, or process which attempts to access an object (e.g. system, data, resource). Also called a principal. |
| **Suite Support** | The ability to properly track individual product vs. multi-product use for software suites of related and interacting products, such as the Microsoft Office Suite, which consists of Microsoft Word, Excel, and PowerPoint. |
| **Symmetric Key Encryption** | A one key method of maintaining encryption keys. The same key is used to encrypt and decrypt information, more than one person when used to protect shared data knows the key. |
| **System** | An assembly of computer hardware, software, or firmware configured to classify, sort, calculate, compute, summarize, transmit, store, control, or receive data. A system may consist of a single stand-alone computer or word processor or tightly coupled multi-processor environment. Also called a computer system, information system, or host. |
| **Telecommunications Equipment** | Electronic equipment that transfers information (voice or data) from one place to another using telephone lines, various frequencies, and/or satellites. |
| **Testing Authority** | The person who authorizes testing of security controls. |
| **Tether** | A device used to physically secure any electronic device (e.g. laptop, printer, etc.) |
| **Token** | A device, usually hand held, to contain unique identity or for generating a unique, cryptographically encoded password. See Two-factor Authentication. |

| Term | Definition |
|---|---|
| **Trading Partner** | Each company that sends and/or receives documents via EDI is referred to as a trading partner. Also refers to any organization or person who does business with SDLC. |
| **Two-factor Authentication** | A method of proving a user's identity by any two of the following means:<br>• Knowledge of a shared secret such as a password or PIN,<br>• Possession of a token, or<br>• A biometric measurement (e.g. fingerprint, voice recognition). |
| **Untrusted Software or System** | System utility or application software that has not been validated or verified as to its integrity or ability to control process or data flow in a secure manner. |
| **Usenet** | A worldwide electronic bulletin board that only includes generally accessible, public newsgroups. Usenet allows SDLC to share General Business Information with a variety of companies. Also known as Netnews. |
| **Value Added Networks (VAN)** | Value Added Networks (V AN) provide additional service beyond the standard store and forward transport function of electronic messaging. A third party to handle common data communication and management functions for trading partners supplies the additional services. This means the trading partner only has to communicate with one communication system. Examples of value added networks include GEIS, IBM Information Network, ORDERNET, TRADENET, and Kleinschmidt. |
| **Wide Area Network (Tier I)** | An electronic information transport mechanism for voice, image, and data which interconnects facilities. |
| **Workstation** | See Computer System |

# APPENDIX C – LIST OF SECURITY RELATED REFERENCES

This appendix refers you to other SDLC related publications related to the use of Computer Resources.

**Policies**

**STANDARD OPERATING POLICIES**

**CORPORATE FINANCIAL POLICIES**

**GOVERNMENT POLICIES**

**STANDARDS**

**GUIDELINES**

# APPENDIX D – EISS CHANGE REQUEST FORM

The EISS Revision Form is to be used to submit any revisions or additions that you recommend for the Electronic Information Security Standards Manual. Please complete the form in full and submit it to your Sector Information Security Council Representative.

**Name** _____ **Date** _____

**Sector/Group** _____ **Mail Drop** _____

**Phone Number** _____ **E-Mail Account**_____

Please specify the chapter/section and page number for which you are recommending an addition/revision.

Chapter/Section _____

Pages _____

**Recommended addition/revision:**

_____

_____

_____

_____

_____

_____

**Reason this addition is necessary:**

_____

_____

# APPENDIX F – COMPLIANCE/EISS COMPLIANCE CHECKLIST

Some controls are not applicable to every situation, and some may present conflict. This appendix describes how to handle non-compliant situations.

**Compliance**

The risk to information and intellectual assets is mitigated primarily by information security. Since most computers and devices share a common data store (servers) and a common communication path (networks), the security of each computer or device affects the overall security of all computers and devices. Exceptions to security requirements and standards must be evaluated by performing a risk analysis, which identifies the threats, estimates the potential for loss, and takes into consideration how much the implementation of the minimum required safeguards cost. If the business chooses to accept the risks inherent with the control weaknesses, all exceptions to security requirements and the reasons for non-compliance, along with any compensating controls must be properly documented and approved. This documentation must be available for department management, system administrators, auditors, and security personnel upon request. At a minimum, it must contain the following:

- Current configuration of the hardware or software being covered by the exception.
- A description of the conflicts (hardware or software), which prevent compliance using, approved methods.
- Documentation showing that the vendors of the conflicting products have been contacted for resolution.
- A statement of when the exception will be reviewed again and/or eliminated.
- A risk analysis summarizing the potential losses and consequences if the information stored in the computers or devices is compromised.
- A description of any compensating controls that are implemented to reduce the risk to an acceptable level. In the case where no compensating controls are acceptable, a short summary of the various controls, which were evaluated, must be included, along with the reasons why each was deemed unacceptable.
- A list of those responsible for the determination and approval of the exception (usually system administrators and their management).

If proper controls (either approved or compensating) cannot be implemented, the computer or device must be disconnected from any SDLC network and it must be marked as non-compliant in a visible manner to alert users that the computer is unacceptable for the storage or processing of sensitive and/or critical data.