Standard Operating Procedure

SOP 1054-01

Title: Non-SDLC Use of SDLC Computers			
Effective Date:	October 1, 2006	Previous Version:	None
Reason for Update:	New SOP		

Owner: Chief Technology Officer Signature/ Date	Location Portland

Objective The purpose this Standard Operating Procedure is to define the process for evaluation and authorization for Non-SDLC staff access to and use of SDLC electronic information, computer systems or networks.

Scope This document establishes the procedures used to determine the appropriate use of SDLC systems including hardware, software and network resources.

Applicable To This policy applies to all electronic information systems of SDLC and its wholly owned subsidiaries as defined by contractual agreements.

Sections
Section 1: Procedure Diagram
Section 2: Policy Statement
Section 3: Metrics
Section 4: Procedure Activities
Section 5: Forms
Section 6: Exemptions
Section 7: Tools/Software/Technology Used

Attachments
Appendix A: Risk Assessment Guidelines
Appendix B: Change Management Request Form
Appendix C: Web Application Maintenance Change Form

Related Procedures
SOP 1005: Release Planning
SOP 1050: Electronic Information Security Standards
SOP 1051: Security Administration
SOP 1052: Protection of Proprietary Information (POPI)

SOP 1053: Appropriate Use of Computer Resources
SOP 1055: Computer Systems Controls

Definitions

The completion of the procedures and evaluations in this policy should provide the following:

a) An evaluation of the benefits that may be provided where the computer can be used to access to customers or vendor computers.
b) Expert opinion(s) of the exposure and risk to SDLC. The SDLC technical or computer security experts should evaluate if proper protection of SDLC data files and software is provided for before access is granted.
c) An assurance that each department concerned has an opportunity to review and comment on the proposal.

Term	Definition
ELECTRONIC INFORMATION SYSTEMS	Computers (including e.g., personal computers, workstations, manufacturing control systems, mainframes, minicomputers, and programmable test equipment), and communication systems (including) e.g., data networks, LANs, routers, electronic mail, and EDI systems)
NON-SDLC PERSON (non-SDLC staff)	An individual who is not an employee of SDLC Inc., such as an agent or employee of another corporation, a consultant or company doing business with SDLC, an employee of a joint venture (which is not contractually obligated to abide by SDLC policies), consortium, trading partner, customer, or supplier and similar operations.
CONTRACT EMPLOYEE	Contract programmers, consultants, hardware and software service engineers, and teachers represent a special class of non-SDLC staff. Through their contract responsibilities, they may be treated as SDLC staff and must comply with all policies and procedures that are applicable. Each Sector and Group must have documented procedures, approved by Sector/Group management, to control contract employee access to SDLC computer systems.
SDLC SPONSOR	The member of the SDLC staff approving the project requiring non-SDLC staff access.

SECTION 1: PROCEDURE DIAGRAM

- None at this time

SECTION 2: ROLES AND RESPONSIBILITIES

Role	Responsibility
Human Resources	Will ensure that new employees receive a copy SOP 1054
LAN and System Administrators	a) Must conduct periodic software licensing and security assessments of all shared systems, including account verification, on at least a yearly basis, retaining records of scope, findings, and corrective actions for at least two years. b) Must provide a unique user ID (computer account) and an appropriate authentication mechanism (e.g., password, security token/card) for each employee having access to SDLC computer resources. c) Must fulfill the administrative requirements for computer resources and information systems assigned to, or controlled by them, as described in EISS and other SDLC policies and standards.
Department Managers	a) Are responsible for the informed interpretation of the provisions of this policy, including the determination of the appropriateness of all non-business uses by employees reporting to them. b) Must ensure employees reporting to them comply with all provisions of this policy. c) Must ensure each employee is properly informed of the individual requirements for compliance with this SOP before authorizing any access to computer resources. d) Must periodically review the access privileges of all employees reporting to them and must report employee status changes that might affect access privileges to appropriate system, network, and security administrators on a timely basis.
Employees and SDLC Users	a) Must comply with all aspects of this policy. b) Must insure that individual user ID(s) (computer accounts) and any other accounts which a user may have access to are protected by adhering to the SDLC user ID and password requirements outlined in the EISS. c) Must comply with changes or amendments to SOP 1053 and the EISS in a timely manner.

Role	Responsibility
Third-Party Access Sponsors	a) Are responsible for informed interpretation of the provisions of this policy, including the determination of the appropriateness of all non-business uses by non-SDLC users sponsored by them. b) Must ensure sponsored non-SDLC users are in compliance with all aspects of this policy. c) Must ensure each non-SDLC user is properly informed of the individual requirements for compliance with this SOP before authorizing any access to SDLC computer resources. d) Must periodically review the access privileges of all sponsored users and must report changes in status of all non-SDLC users that might affect access privileges to appropriate system, network, and security administrators on a timely basis.

SECTION 3: METRICS

- None at this time

SECTION 4: POLICY STATEMENT

Section	Policy Description
4.1	The use of SDLC information systems by non-SDLC organizations and persons is a practice that must be allowed only under carefully controlled conditions including compliance with all applicable security policy, control standards and government regulations.
4.2	In order for non-SDLC staff to gain access to a SDLC information system, the following criteria must be satisfied: A legally binding contract, signed by a duly authorized member of the SDLC staff must be in force between SDLC and the employer for the non-SDLC employee. In the case of individuals, the contract, signed by a duly authorized SDLC staff member, must be in force between SDLC and the individual. In the case of a Joint Venture, the agreement must be between duly authorized individuals in each entity. This contract must include a non-disclosure statement and intellectual property rights language as approved by the applicable Corporate/Sector/Group Intellectual Property and Human Resource Departments. found in Appendix I, unless the organization meets the Sector/Group requirements for contract employee management. In addition, joint ventures which are contractually obligated to abide by SDLC policies, do not have to prepare risk assessments. This assessment must be approved by the sponsor manager, the Sector/Group Internal Control Manager and the Sector/Group Information Security Manager before access is granted. The sponsor shall retain the original assessment form and provide it to their successor.
4.3	The specific non-SDLC individual must be bound by a document that includes a non-disclosure agreement, a statement that she or he will abide by SDLC's information security policies, and any other documents required by Sectors and Groups.
4.4	The computer user account request form must include written approval of the sponsor, the sponsor's manager, and the data owner(s). This account form must include the following references to contract with the non-SDLC entity: contract title or reference number, contract commencement date, and contract expiration date. The user account must be disabled no later than the termination date of the contract.
4.5	The user account form should be retained by the system administrator until one year after the contract terminates.
4.6	When it is determined that access should be allowed to SDLC's business data and computer resources, it will be the responsibility of the originating department to prepare the non SDLC Computer User Proposal.
4.7	This policy applies to non-SDLC access granted after October 1, 2000.

SECTION 5: FORMS

- None at this time

SECTION 6: EXCEPTIONS

- None at this time

SECTION 7: TOOLS/SOFTWARE/TECHNOLOGY USED

- None at this time

Appendix A: Risk Assessment Guideline

Guideline For Risk Assessment Process For Non-SDLC Use
of SDLC Electronic Information Systems

Overview

A procedure is described to ensure that a risk assessment has been completed and documented for non-SDLC staff use of SDLC's electronic information systems. This guideline is to ensure that all managers that recommend and approve such access are fully cognizant of the benefit/risk assessment before committing to provide access to SDLC's computer systems. A risk assessment should be completed prior to authorizing any non-SDLC staff use of our electronic networks and systems. Non-SDLC staff members are required to comply with SDLC's security policies and standards.

Introduction

The use of SDLC Information Systems by non-SDLC organizations and persons is frequently required to support our business units. SDLC has a major investment in proprietary information stored on, processed by, or accessed via these information systems.

There are significant risks associated with allowing non-SDLC individuals to use our electronic information systems and networks. Non-SDLC groups include contractors, joint venture partners, trading partners, a consortium, customers, suppliers, and temporary employees.

This guideline will assist an organization in preparing a risk assessment
to authorize access to SDLC's electronic information networks and systems by non-SDLC staff.

Evaluation Procedure

The risk assessment is prepared by the sponsoring SDLC organization that is proposing access for a non-SDLC employee. The sponsoring manager, the data owner(s), internal controls and the information security function before access is granted must approve this assessment. The sponsor will retain the original assessment form.

Risk Assessment Check List

A risk assessment should include the following:

- General Information
- Proposal prepared by (Sponsor's name)
- Date Prepared
- Company Name
- Company Address
- Business Function
- Company's relationship with SDLC
- Contract Title or Reference Number
- Date Service Agreement or Contract Signed (to include non-disclosure agreement and intellectual property language)
- Date Agreement/Contract Ends
- Connectivity Requirements

Detailed Information on the business requirement risks and plans to mitigate the risks

- Describe the business reason for the request.
- How does it support the strategies of the business unit?
- What are tangible, quantifiable benefits to SDLC?
- What are non-tangible benefits to SDLC?
- Provide the name of the application(s) and the POPI classifications of the information to be accessed.
- Describe the planned information systems access
- Dial-in access
- Leased line or direct connection
- On-Site (peer-to-peer)
- Wireless or satellite

Describe the risks of compromise of the SDLC information.

- Fraud
- Disclosure of intellectual property -Compromise of information integrity
- Describe how information will be protected and access controlled.
- Local access control
- Remote access controls
- Anti-virus
- Regular account reviews
  Compliance with EISS and SIC

- Periodic audits and self-audits
- Individual non-disclosure agreements -Notification procedure to end access
- Management and data owner approval of all access
- Notification/ documentation provided to LAN administrator(s) of any cross business unit access

Documentation Required for Individual Contract Employee

- Name of Non-SDLC User (work location/phone number/email)
- Sponsoring Manager
- LAN-Administrator
- Type of Required Access (Remote or On-site)
- POPI Classification for Information to be Accessed
- End Date for Required Access

Appendix B: Change Management Request Form

- See Attached

Appendix C: Web Application Maintenance Change Form

- See Attached