Standard Operating Procedure

SOP 1053-01

Title: Appropriate Use of Computer Resources			
Effective Date:	October 1, 2006	Previous Version:	None
Reason for Update:	New SOP		

Owner: Chief Technology Officer Signature/ Date	Location Portland

Objective To define the policy and responsibilities necessary to ensure confidentiality, security and appropriate use of SDLC's information assets, computer resources and information systems. To ensure that SDLC and users of SDLC computer resources are in compliance with the applicable license agreements for software used for SDLC business.

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 and operating procedure applies to all employees using any computer resources of SDLC or its subsidiaries worldwide. This policy also applies to non-SDLC users of SDLC computer resources. Non-SDLC users who only use computer resources that are intended for public access are exempt from the provisions of this policy.

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 None

Related Procedures SOP 1005: Release Planning

SOP 1050: Electronic Information Security Standards
SOP 1051: Security Administration
SOP 1052: Protection of Proprietary Information (POPI)
SOP 1054: Non-SDLC Use of SDLC Computers
SOP 1055: Computer Systems Controls

Definitions

For purpose of this SOP, "SDLC Computer Resources" (CCR) means computers, peripherals, printers, plotters, scanners, modems, internal and external networks, and other computer communication devices owned or leased by SDLC, whether used by employees, agents of SDLC, or non-SDLC staff users.

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 1053
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.

Role	Responsibility
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.
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	SDLC Computer Resources may only be used for purposes which effectively and efficiently support Company business goals and objectives, or for non-business purposes which are approved by management. Any questions regarding approved use should be referred to the applicable department manager or that manager's designee. The use of SDLC computer resources must comply with the provisions of other policies, such as the Code of Conduct, non-disclosure agreements, Human Resource policies, employee handbooks and applicable laws. The following are examples of some, but not all, inappropriate uses: communicating in a defamatory, derogatory, or harassing manner, infringing on intellectual property rights (including copyright, trademark and servicemark) , transmitting chain letters, or information which contributes to a hostile or unproductive workplace, use for any illegal purpose, use in excess of granted authority, or creating, storing, viewing or transmitting offensive graphics.
4.2	All software stored in or executed on SDLC computer resources must be used in accordance with applicable license agreements, and must be properly licensed, or owned by SDLC, or in the public domain. Public domain and shareware software are allowed only after ensuring the necessary rights have been acquired and any required fees have been paid.
4.3	Each software license contains terms and conditions that are unique and which must be carefully reviewed and complied with. Unless otherwise stated in an applicable license, for internal assessment purposes, each software license is presumed to be for a single copy, operating upon a single computer or processor. Unless otherwise authorized by the terms of an applicable software license or other legal means, the following are prohibited: a) The production of or distribution of unauthorized copies of any software; b) Transfer, assignment, or sale of licensed software to any non-SDLC employee including clients, customers, and others; c) Transfer, assignment, or sale of SDLC-owned software to any non-SDLC employee including clients, customers and others; d) Shared usage of licensed software across local and wide-area networks; e) Export or import of any governmentally-controlled software (such as software encryption) to or from unauthorized locations or persons without appropriate licenses or permits; and f) Duplication of licensed software documentation in whole or in part.

Section	Policy Description
4.4	It is the policy of SDLC to protect confidential, sensitive or critical information owned by SDLC or in SDLC custody. Sensitive information must be properly classified, marked and protected according to SOP 1052, Protection of Proprietary Information (POPI) , or other SDLC information security policies.
4.5	Information and software residing on computer devices, peripherals and removable storage media must be secured to prevent unauthorized access and theft. Standards for securing user IDs (computer accounts) and adhering to the SDLC user ID and password requirements are outlined in the EISS.
4.6	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.
4.7	All computing resources used to process or store sensitive or critical information, either owned by SDLC or in SDLC custody, must have security and virus detection software installed and appropriately configured in accordance with EISS.
4.8	The use of software (especially public domain software and software downloaded from external networks or computer bulletin boards) must be preceded by a satisfactory virus scan, functional evaluation, and test in a non-production, isolated environment.
4.9	Each user must be given a copy of the policy and is expected to read and understand the policy before using SDLC computing resources.
4.10	All employee and non-SDLC users must comply with this policy, including the specific responsibilities summarized below or contained in the EISS and other applicable policies and standards. Violations of this policy by any individual may result in disciplinary action in accordance with SDLC Human Resource Policies and/or appropriate legal action.
4.11	SDLC reserves the right to access data created, stored or transmitted using SDLC computer resources as deemed necessary and approved by SDLC management, conducted in compliance with applicable laws, and required in the support of SDLC business.

SECTION 5: FORMS

- None at this time

SECTION 6: EXCEPTIONS

- None at this time

SECTION 7: TOOLS/SOFTWARE/TECHNOLOGY USED

- None at this time