PROCEDURE OVERVIEW

Security Administration provides an overview to the areas of security control activities within the SDLC.com business environment. The ***Security Administrator*** is the individual charged with identifying, communicating, monitoring and addressing issues and concerns that pose threats to computer and intellectual assets. Threats are defined as any form of intentional or unintentional access to confidential or sensitive materials by an unauthorized individual.

The ***Security Administrator*** oversees and maintains system access profiles. System access requests are compared to pre-approved profiles as part of the request approval process. Approved access is logged whenever it is considered an exception. On a quarterly basis, the exception log is analyzed and recommendations for improvement are presented to management. A periodic review of profiles is performed.

Security Administration addresses the disposal of paper and electronic media, any of which may include confidential data. In addition, it addresses third party requests for information and the process to authorize the release of materials.

The Security Administration procedure defines the rules under which documents are to be annotated to show that they are the property of SDLC.com. All materials are to be consistently treated as though they contain confidential or sensitive information.

Procedure Owner: Manager of Operations

Table of Contents

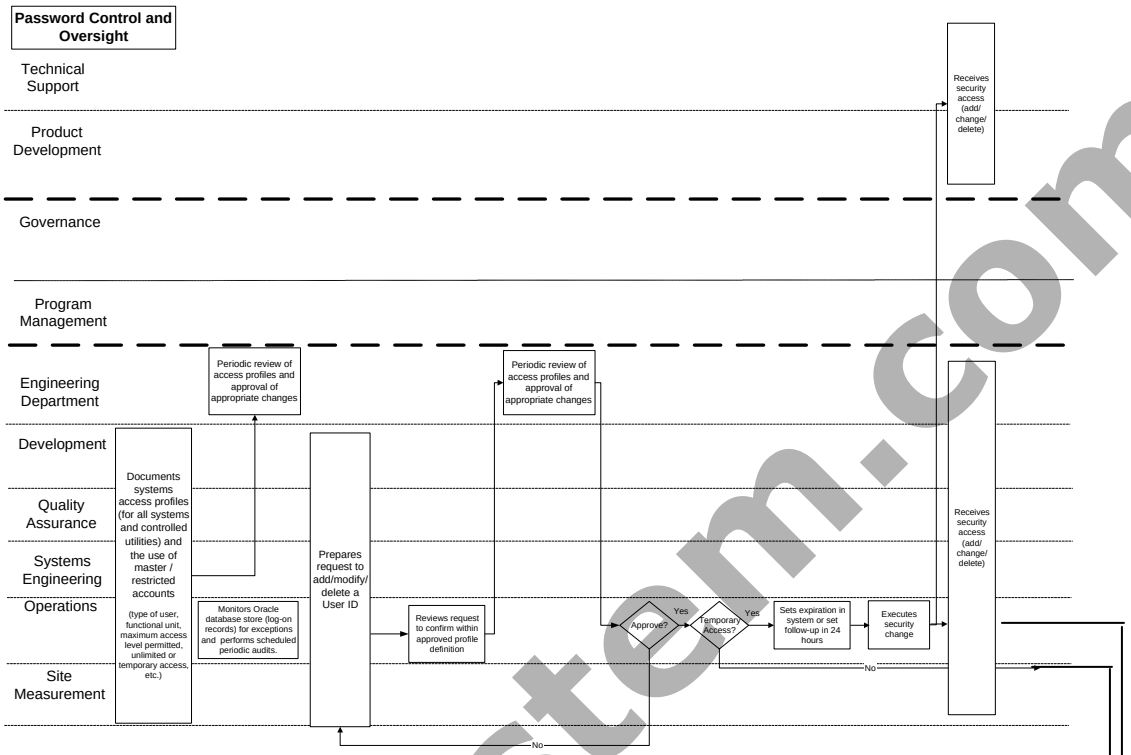
REVISION HISTORY

Version	Date	Author	Description

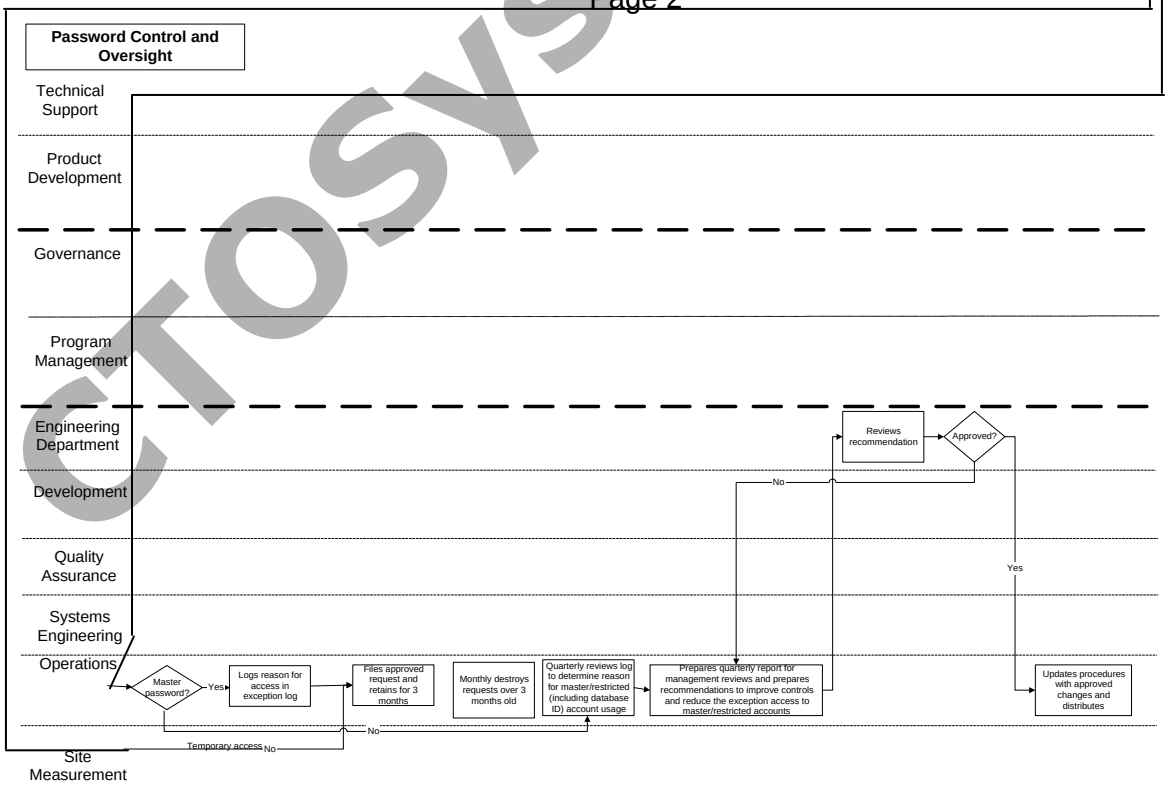
Distribution List:
Chief Technology Officer, Bob Stewart, Engineering Department
Manager of Operations, Engineering Department
Manager QA, Engineering Department
VP Systems, Engineering Department
Security Administrator, Engineering Department

PROCEDURE DIAGRAM

Page 1



Page 2



ROLES AND RESPONSIBILITIES

Security Administrator

The **Security Administrator** is charged with identifying, communicating, monitoring and addressing issues and concerns that pose threats to computer and intellectual assets. This person oversees and maintains systems access and performs periodic reviews of profiles. In addition, the **Security Administrator** prepares quarterly reports and makes recommendations for improvement to management.

METRICS

Cycle Time

The amount of time required to complete all steps in the creation/maintenance of a user ID from the time a request reaches the **Security Administrator** through delivery of the executed maintenance to the individual.

Advisories

A list of security advisories published each month along with its source and the time consumed in preparation and distribution.

Special Events

The number of occurrences and amount of time spent on security events/investigations each month. Each event will have a management report on file.

Change Agents

Individuals who analyze a process and recommend ways to improve it, regardless of whether or not the recommendation is implemented. The person's name will be reported to Engineering Department management and will receive recognition for their effort to compress cycle times and/or improve quality.

PROCEDURE ACTIVITIES

Security Profiles

Access to SDLC.com system environments is a "Right" that permits an individual to perform the duties associated with a particular job. Users are given access rights based on their job responsibilities and the training or knowledge they possess. Knowledge and skills are to be evaluated after each major enhancement to ensure they are current. The ***Security Administrator*** is responsible for verifying individual skill sets with appropriate management.

Profiles are defined as follows:

Area / Unit	**System Environment**					
Engineering	**Development**	**QA**	**System Certification**	**FOA/ Beta**	**Staging**	**Production**
Sustaining Development	RW	RO	RO	RO	RO	None
Advanced Development	RW	RO	RO	RO	RO	None
Strategic Development	RW	RO	RO	RO	RO	None
Quality Assurance						
Applications	RW	RO	RO	RO	RO	None
Databases	RO	RO	RO	RO	RO	RO
Systems Engineering						
Applications	RO	RO	RO	RO	RO	RO
Databases	Exception	Exception	Exception	Exception	Exception	Exception
Hardware	Full	Full	Full	Full	Exception	Exception
MIS Database	RO	RO	RO	RO	RO	RO
SDLC.com Internal Departments						
Content (Content Utilities)	None	None	None	None	W *	W
Technical Support	None	None	None	SU	SU	SU
External Entities						
Hosting	None	None	None	Full	Full	Full
TMG (Content Utilities)	None	None	None	None	W *	W

Legend:
RW = Read / Write
RO = Read Only
Full = Unrestricted
Exception = Full access with use restricted to request fulfillment
W = Write (Direct write of Content to Production Database)
W* = Write (Direct write of Content to Staging Database with automatic content update to the production environment.)
SU = Super User Utility to assist Web users with ID issues. Audited through review of database logs.
None = Standard Web access only. No access to applications, databases or hardware.

Sandbox environments are excluded from this procedure. Owners have control over their own environments.

Monitoring of direct content writes to production is required.

	Access Areas			
Area	**Servers**	**Resonate**	**Database**	**Network / H/W**
Network	**X**	**-**	**-**	**-**
DBAs	**-**	**-**	**X**	**-**
Unix	**X**	**-**	**-**	**-**
Feeds	**X**	**-**	**-**	**-**
OCC	**X**	**-**	**-**	**-**
Release Engineering	**X**	**-**	**-**	**-**
Ops Engineering	**X**	**X**	**-**	**-**
Ops Management	**X**	**X**	**X**	**X**

Legend: X = Normal access rights for individual trained and demonstrating skills
- = Situational exceptions requiring security to be enabled. Individuals may act in the capacity of a backup for the primary individual without being a member of the specific area.

Situational access is subject to audit review. Situational access requires that actions performed be documented and communicated to the appropriate areas within the Engineering Department. The manager who authorized access is responsible for ensuring that documentation and communication is completed and distributed in a timely fashion.

Password Control and Oversight

User IDs and passwords will be unique and assigned to one individual. Group logon IDs will be prohibited. This not only increases accountability, but provides the means to audit activities.

The process flow on page 4 provides a high level view of the Security Administration procedure for Password Control and Oversight. Access to systems is defined first by the role of the unit to which an individual is hired or contracted. Each unit has a profile defining the privileges associated with the roles and responsibilities of the normal work requirements for that unit. These profiles are defined above. Deviations from a unit profile require a compelling reason for permanent access. Temporary access may be granted based on circumstances and the approval of appropriate management.

The ***Security Administrator*** has primary responsibility for establishing, modifying and removing access as approved by the ***Manager of Operations***. ***Department Managers*** (and Human Resources) are responsible for timely notification to the ***Security Administrator*** of termination, promotions, transfers and new hires. The ***Security Administrator*** will immediately disable the terminated individuals access.

Due consideration must be given prior to the granting of access rights to a consultant. The ***unit manager*** is responsible for performing a knowledge assessment and an education process regarding SDLC.com's standards and technology environment, prior to allowing the individual access to the SDLC.com systems. Access rights should be limited to the consultant's engagement scope.

Each request for a security change is routed sequentially through the following steps.

1. ***Requesting Department Management*** completes and authorizes the **Security Change Request Form** (Appendix 1). In cases where exceptions are being requested, documentation supporting the request must be provided, as well as the duration of the requested access privilege.
2. Request is forwarded to the ***Security Administrator*** for comparison to approved profile. (Requests will normally be processes within four (4) business day hours.) Based on the results of this comparison the request is either:
   - Delivered to the ***Manager of Operations*** for Approval
     - Request is within approved profile definitions
     - Request is outside approved profiles but has supporting documentation
   - Returned to ***Requestor*** or ***Requesting Department Management***
     - Request is outside approved profiles and does not have supporting documentation
3. Approved requests by the ***Manager of Operations*** are implemented and steps 4 through 6 are executed. Rejected requests are returned to ***Security Administrator*** for return to ***Requestor*** with an explanation for the rejection.
   - ***Requesting Department Management*** may appeal the rejected request by reviewing the reason with the ***Manager of Operations.*** Should acceptable resolution not be achieved, the ***Senior Manager of the Engineering Department*** will arbitrate. That decision will be final.
4. Is the request for *Temporary Access*?
   - Yes – the ***Security Administrator*** sets password expiration in the system or schedules follow-up in 24 hours (next business day) and proceeds to step 5
   - No – executes step 5
5. Is a Master ID involved in the request (outside standard profile)?
   - Yes – ***Security Administrator*** logs the request and reason in an exception log and proceeds to step 6
   - No – executes and files the request; proceeds to step 6
6. The ***Security Administrator*** meets with the ***Requestor*** that access privileges are now available. The ***Requestor*** signs the **Security Change Request** form acknowledging receipt.

Quarterly Report

1. The ***Security Administrator*** analyzes the exception log to determine trends and reasons for requests. These findings are used to prepare a quarterly report. The report includes recommendations for root cause remediation, changes to standard profiles, process improvement, etc.
2. The ***Manager of Operations*** reviews the ***Security Administrator's*** recommendations:
   - Approved recommendations initiate the following process:
     - Procedure updated following **DOCUMENT GOVERNANCE PROCEDURE**
     - Recommendation directed to the appropriate ***Unit Management*** for consideration
     - ***Manager of Operations*** or ***Security Administrator*** champions the change in process
   - ***Manager of Operations*** requests for additional analysis and/or additional detail are handled by the ***Security Administrator*** in an appropriate and timely manner.

The ***Security Administrator*** reviews database access logs monthly to determine when exception access, unusual access or other events occurred which warrant additional review. The ***Security Administrator*** performs the necessary review and promotes findings to the

Manager of Operations at the time of discovery or as part of the quarterly report depending on severity.

The ***Security Administrator*** is responsible for ensuring that temporary access permissions are disabled at the end of the authorized period. The default period is one business day.

The ***Security Administrator*** has the responsibility to disable access to any individual when that individual's actions create a perceived threat to the systems environment. This responsibility will be executed without regard to the individual's title. Due diligence will be undertaken prior to taking this escalation avenue. In the event that the reason for the individual's action can not be determined and ***Operations Management*** is unavailable for council, the ***Security Administrator*** will disable the users account. Determination of the event and a report will be generated by the ***Security Administrator*** and distributed to both the ***Manager of Operations*** and ***the Senior Manager of the Engineering Department***.

PROTECTION OF INTELLECTUAL ASSETS

The **CMGI Employee Handbook** used by SDLC.com addresses the protection of intellectual assets in the "Corporate Code of Ethics and Conduct Policy" section; specifically sub-sections:

- Protection of Assets of CMGI
- Confidential Information
- Conflict of Interest
- Sanctions for Breach of Ethical Standards

Each ***employee*** must sign a non-disclosure agreement at the time of hire. The terms and conditions of that agreement will be enforced.

Document Notices

Each ***employee*** creating documents for internal use with confidential information or containing intellectual asset descriptions or definitions shall include a footer throughout the entire document stating "Confidential - Property of SDLC.com." This applies to all documents that contain naming conventions used in coding and network configuration.

Materials created for clients are to have "Copyright, SDLC.com MM/YYYYY" (Month and Year) on each page.

Client/Partner Requests for Information

Any request for information from a client or partner that extends beyond what an employee considers regularly provided information will be honored only after authorization by ***Department Management***.

Authorization means:

- Approval to compile the information within a defined scope approved by management.
- Review and approval of materials prior to release.

Materials designated sensitive that will be released to clients or partners will have a cover document stating that the materials are “Intellectual Property of SDLC.com.” All provided materials will have a footer on each page as stated under the Document Notices section above. The individual authorizing the release of materials will maintain a description of the materials released, with their specific source.

Input to Development and Configuration Standards

The ***Security Administrator*** is responsible for maintaining a dialog *with* ***Development, Operations and Configuration Functions*** within the Engineering Department and ***Content Staff*** in the Product Department. The ***Security Administrator*** will generate an advisory announcement each time a potential threat is discovered. Compliance with these advisories is the responsibility of staff in ***Development, Operations and Configuration Functions*** within the Engineering Department and ***Content Staff*** in the Product Department. An individual performing peer review and/or validating application/content has responsibility for ensuring the adherence to advisories.

General Guidelines

- Never encode sensitive information in a client-side script such as JavaScript.
- HTML should use “Post” versus “Get” methods, when possible.

PAPER DISPOSAL

Documents generated through the normal course of performing job-related duties must be considered to contain confidential information. As such, each employee is expected to consider this when disposing of paper.

DISPOSAL OF ELECTRONIC MEDIA

Any electronic media disposed of is to be rendered unusable. This requires that storage media be physically destroyed or passed through a magnetic field to erase content or be reformatted using a utility that writes a constant stream of values to the disk surface.

OFF SITE STORAGE OF BACKUP MATERIALS

Any materials stored off-site will be placed in a locked container. When backup materials represent a systems environment, storage media will contain all necessary instruction to restore the environment, including passwords and current disaster/business recovery instructions.

Operations will maintain a log of all off site materials.

FORMS

- Security Change Request Form

EXCEPTIONS

- Sandbox environments are excluded from this procedure.

AFFECTED/RELATED PROCEDURES

- **DOCUMENT GOVERNANCE**

TOOLS/SOFTWARE/TECHNOLOGY USED

- Oracle Database Store
- Operating System Security Functionality
- Application Security Functionality

APPENDIX

- Appendix 1 - Security Change Request Form

Appendix 1 - Security Change Request Form

Security Change Request Form

Name: _____ Unit: _____

Title: _____ Required Date: _____/_____/_____

Requested Access: (Circle Requested Level)

Environment	Application	Database	Hardware
Development	RO / RW / Full	RO / RW / Full	RO / RW / Full
Quality Assurance	RO / RW / Full	RO / RW / Full	RO / RW / Full
System Certification	RO / RW / Full	RO / RW / Full	RO / RW / Full
FOA (Client Acceptance Test)	RO / RW / Full	RO / RW / Full	RO / RW / Full
Production	RO / RW / Full	RO / RW / Full	RO / RW / Full

Signature of Requestor: _____ Request Date: _____

Approving Manager has assessed the individual's knowledge and skills and certifies that the named individual meets all requirements for the security access level requested. For access beyond development, the approving manager has assessed the individual's knowledge of SDLC.com's technical environment and it meets all requirements for the security access level requested.

Approving Manager: _____ Request Date: _____

Request in compliance with approved security access profiles? Yes / No (Circle one)
If No, is substantiating documentation attached? Yes / No (Circle one)

Security Administrator: _____ Date Received: _____

Authorizing Manager: _____ Date: _____

Secuirty Access Information:

User ID: _____ Date Executed: _____

Verified by: _____ Date: _____

Acceptance Signature (User ID delivered and accepted by):

_____ Date: _____

By signing and accepting access to SDLC.com systems environment I warrant I have completed and returned an executed non-disclosure agreement.