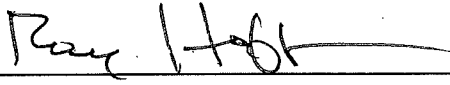


Title Utility Account Access – Consolidated Customer Service System (CCSS)	Number CS-106.2	Rev. no. 0
Responsibility Customer Service Branch	Supersedes N/A	Pages 3
SPU Director's Approval 	Effective Date November 15, 2012	

1. PURPOSE

This procedure establishes direction for determining, requesting, changing, removing, and reviewing employees' access to the Consolidated Customer Service System (CCSS), also known as Banner. It conforms to the policy CS-106, Customer Utility Account Transactions, part B.

2. DEFINITIONS

The following includes key terms and examples that describe and provide background on how security is set in CCSS:

- *CCSS Forms*: Access to various billing actions in CCSS is compartmentalized into discrete functions via the use of Forms. For example, Form UAAMADJ, which stands for "Adjustment Posting," is used to adjust an account. If UAAMADJ were the only Form the user had access to, then adjustment postings would be the only action the user could perform. See CS-106.2b, *CCSS Security Classes and Forms*.
- *CCSS Security Classes*: Security Classes are used for controlling or limiting access by users in CCSS. Each Security Class has a defined list of Forms assigned to it which allows read-write access. A Form can appear in multiple Security Classes. A user may need more than one security class. See CS-106.2b, *CCSS Security Classes and Forms*.
- *Security Class Roles*: Categorizations of security classes delineated by job function. For example, security class BAN_MTN_CUST-RESP_C includes access to a series of Forms that SPU call center employees use.
- *BAN_MTN*: Security Classes beginning with BAN_MTN are read-write. MTN stands for maintenance.
- *BAN_QRY*: Security Classes beginning with BAN_QRY are read-only. QRY stands for query.
- *Company*: The utility associated with a customer account prefixed by either 01 for Seattle City Light or 02 for Seattle Public Utilities. Security Classes are established separately and independently for each company.
- *RQA Auditor*: A staff member in the Risk and Quality Assurance Division responsible for coordinating CCSS access for SPU.

3. PROCEDURE

A. Determining Access Type

Utility account access is only granted to employees having a business need; in other words, the employee's job duties will require them to access and / or make transactions to the billing system.

1. Managers are responsible for understanding the different Security Classes and Forms, and the relevant job duties of their employees, in order to determine the type of access to grant employees.
2. Managers will determine and set access levels separately for each Company, recognizing that an employee's access to one Company may be different than the other based on job duties.

B. New User Application

1. To request access for a new user, Managers will:
 - a) Select the appropriate Security Class for the user based on their job duties.
 - b) Complete an *CCSS Access Form* (form CS-106.2a) available from SPUweb IT Forms or the Policies, Procedures and Rules webpage.
 - c) Have the employee read, sign and date the *Confidentiality Agreement Seattle City Light & Seattle Public Utilities* (form CS-106.2c).
 - d) Sign the *CCSS Access Form* (form CS-106.2a) and give it to the Division Director.
2. Division Director will:
 - a) Sign and approve the *CCSS Access Form* (form CS-106.2a).
 - b) Send both forms to the CCSS Service Desk and to the RQA Auditor; e-mail is preferred.
 - c) Retain the original documents in the supervisory file so long as the employee reports to the division.
3. City Light will notify the new user, Manager, Division Director, and RQA Auditor of user ID and password.

C. Change or Remove User Access

1. The following conditions require changing or removing user access:
 - Change in job duties
 - Beginning of an Out-of-Class assignment
 - Ending of an Out-of-Class assignment
 - Separation from employment
 - Management decision

These changes must be requested on or before the date of the change in job status.

2. The Manager will complete *CCSS Access Form* (CS-106.2a) and mark the necessary changes. Manager will sign and forward the form to the Division Director for approval.

3. The Manager will send form to CCSS Service Desk and the RQA Auditor; e-mail is preferred.
4. The Division Director will retain the original documents in the supervisory file so long as the employee reports to the division.
5. City Light will notify the Manager, Division Director, and RQA Auditor when request is complete.

D. Access Review

On a semi-annual basis, a review of the CCSS user access list will be conducted as follows:

1. The RQA Auditor will provide a copy of the current access list and Security Class structure to Division Directors at the end of second and fourth quarters.
2. The Division Director will verify the accuracy and completeness of the access list and notify the RQA Auditor of any discrepancies and changes.
3. The Division Director and the Manager will review the list of Security Classes and Forms to ensure that access types meet the business needs.
4. The RQA Auditor will assist in obtaining changes to Security Classes and Forms and will coordinate with City Light.

4. AUTHORITY/REFERENCES

- CS-106, Customer Utility Account Transactions
- CS-106.2a, CCSS Access Form,
- CS-106.2b, CCSS Security Classes and Forms
- CS-106.2c, Confidentiality Agreement Seattle City Light & Seattle Public Utilities