Customer Service Center Operations Manual

Customer Service Center Security Functions
CSCOM-204

Original Date: 09/22/1987
Revision Date: 02/10/2024

DESCRIPTION

This procedure provides Customer Service Representative (CSRs) and management/designee guidance on daily operational, building, personal, and physical security.

FRONT COUNTER CSR—OPERATIONAL SECURITY

CSRs are required to comply with these requirements at all times to ensure the physical and operational security of the CSC and to guard against fraudulent activity.

OPERATIONAL SECURITY

1. Remove all personal possessions from the front counter window (including but not limited to: coats, cell phones, pagers, purses, backpacks, briefcases, magazines, food, chewing gum).

Items Allowed on the Front Counter[1]	
Pens	Note Pad
Stapler	Teller Stamp
Staple Remover	Ink Pad
Paper Clips	
Drinks with sealable tops, stored in a cabinet or drawer and kept out of customer view.	

[1] *Management may modify items allowed on the front counter to enhance efficient operations.*

2. Lock personal computers (PCs) whenever required to leave for extended periods of time (e.g. lunch, breaks, road skills testing) and unlock when returning.
   - Locking computers may be accomplished by:
     - Press CTRL+ALT+DELETE.
     - Click "LOCK COMPUTER"
3. Ensure drawers containing assigned stamps, decals, and monies are locked whenever the CSR is:
   - Unable to view/monitor their workstation
   - Absent from the work station for any extended period of time.
4. CSRs are responsible for assigned stamps, decals and monies throughout the business day, until returned to, and accounted for, by CSC management or designee.
5. Wear DMV Employee Name Tag throughout the business day.
6. Wear DMV Employee ID so that it is always visible throughout the business day.
7. Remove customer clipboards and stow away from the front counter after customer is called to the front counter.
8. CSC personnel are **prohibited** from:

- Processing transactions under another employee's login ID, sharing PINs, and sharing passwords.
- Accessing their own records, friend's records, or records of immediate family members (spouse, parents (including step-parents), grand-parents, children (adopted and step-members), grandchildren, siblings, in-laws, etc).
- Processing a transaction for themselves or their immediate family members.
    - If a CSR or Manager brings work to be processed for family or friends, they must notify a member of management. Management will determine whether the transaction can be processed and assign it.
        - Both the management and requesting CSR must complete the "Family and Friends Transaction Log" (CSMA-76) before work is completed.
    - CSRs needing a transaction processed for themselves must notify management of work desired to be completed and management will assign the work as needed.
        - CSC employees renewing their vehicle registration(s) and/or driver's license may choose between the following 2 service options:
            - Renewing online. CSC employees must notify management of their need to renew their registration/license. Management will establish a time and place (this MUST be away from the front counter) for the CSR to process their transaction during the business day.
            - Renewing in a CSC.
- Inquiring on records or processing transactions for co-workers unless assigned and authorized by CSC management.
    - If a Customer Service Representatives (CSR) or manager brings work to be processed for family or friends, they must notify a member of management. Management will determine whether the transaction can be processed and assign it. Both the management and requesting CSR must complete the Family and Friends Transaction log **before** work is completed.
- Directly admitting (or otherwise avoiding Q-Flow ticketing) without permission from management.
- Accessing customer's records without having proper authorization or legitimate business needs.
    - CSRs must receive manager approval before accessing a customer's record when the customer (or authorized representative) is not present in the CSC.

      EXCEPTION: Management is permitted to make an exception for dealer work.
- CSC personnel are prohibited from accepting gifts of any sort from customers, vendors or others.
- CSC personnel may not manipulate policies or use system loopholes or to assist customers in avoiding costs or achieving results to which the customer is not entitled.

9. CSC personnel may only use messaging software for work related responsibilities.
10. CSC personnel are required to notify management if their license becomes suspended or revoked (and job duties require a valid driver's license).
11. CSRs must ensure to notify management if they determine they have made a processing error (both revenue and non-revenue transactions).
    - CSRs and Customer Service Center (CSC) management may NOT call customers if a revenue discrepancy is discovered.
12. CSRs must receive management approval before processing a customer's work if the customer (or authorized representative) is not present in the CSC.

    EXCEPTION: Management is permitted to make an exception for dealer work.
13. Internet usage is limited to DMV IT Security Policies and acceptable use policies.
14. Employees must notify a member of management--not coworker or security-- if they need to make an unscheduled departure from the CSC or will be arriving late.
15. CSC personnel must complete and sign the "CSC Employee Operational Security Acknowledgement" (CSMA-88) on an annual basis.

Return to top of page

CSC MANAGEMENT/DESIGNEE—OPERATIONAL AND BUILDING SECURITY

CSC Management is responsible for the overall security of the Customer Service Center and its contents.

OPERATIONAL SECURITY

1. Ensure Front Counter CSR complies with all Front Counter CSR responsibilities listed above.
2. Count CSR petty cash bags, office cash, and revenues (including pickups) out of public view. They may be counted at the window, or at the back counter but MUST be out of direct view of the public.
3. Ensure:
   a. Change fund is kept in a locked area outside the security closet to minimize the number of entries into the security closet.
   b. Dealer transport plate inventories are kept locked at all times. CSCs may use the security closet, a security cabinet in stock room, or another secured location. Only CSC management and keyholders can access tag storage.
   c. VISTA/IFTA inventory is kept either in a locked area outside of the security closet, or in the security closet.
   d. All funds are locked/secured in the safe at the end of each business day.
4. Lock the following during **non-business hours**:

Items to Be Locked During Non-Business Hours	
Blank Title Documents	Permits
Decals	VIN Plates
CSR Stamps	Dealer Transport Tags
EZ Pass Transponder	Blank VDH Documents
Handicap Temporary Placards	

5. If a hardcopy of the CSC Crisis Action Plan Manual is maintained in the CSC, it must be kept up to date. If the manual is accessed exclusively via the intranet, a hardcopy is not required.
6. Ensure all CSC employees complete and sign the “CSC Employee Operational Security Acknowledgement” (CSMA-88) on an annual basis.

INTERIOR BUILDING SECURITY

1. Keep all doors, other than the main entrances, locked at all times. Locked doors may be used as emergency exits, if needed.
2. Ensure all restrooms, breakrooms, stock rooms, and interior offices are not occupied prior to the last employee leaving each day.
3. Verify the safety and security of all credit and debit card data that is collected, stored, and transmitted by the CSC following the guidelines below:
   - Physically inspect all card payment terminals monthly for fraudulent faceplate devices or “skimmers” placed over the original faceplate, and for other signs of tampering or modifications that would compromise the credit or debit card payment process,
   - Identify any third-party persons claiming to be repair or maintenance personnel prior to granting access to modify or troubleshoot payment card terminals,
   - Advise staff that NO payment card equipment is to be installed, replaced, or returned without prior consent from management and the required verification process,
   - Report suspicious behavior, device tampering, or unauthorized substitutions immediately to your District Manager.
4. Test the alarm system (including panic buttons) on a monthly basis. Retain documentation on file at the CSC with dates of testing (refer to CSCOM-1101).
5. Ensure the keypad alarm system is adequate for the CSC's needs. The system should allow each employee to have a unique passcode.

6. Ensure each employee with access to the CSC has a unique secret passcode.
7. Ensure different locks are used on all CSR drawers, and no two drawers share the same key.
    - Duplicate CSR drawer keys must be locked in the security closet.
8. Obtain an Event Log from the CSC's security alarm company and review the log monthly for potential security violations or discrepancies. Retain the log on file at the CSC (refer to CSCOM-1101).
    - CSC Managers may either:
        - Login and review the event log online (if available), or
        - Electronically save (to the CSMA folder on the S: drive) the event log monthly if unable to access the event log using a login, or
        - Sign and retain the physical report on file at the CSC (refer to CSCOM-1101) if unable to login or electronically save the event log.
    - If a security violation or discrepancy is discovered, notify the District Manager and await further guidance.
9. Email the district office monthly indicating the alarm systems (including the panic buttons) are operational and the event logs have been reviewed.
    - The district office will notify CSMA Director monthly that all equipment has been reviewed and operational.

    <<<<<REVISION

10. Ensure that all visitors and guests coming in and out of a CSC sign the “CSC Visitor Sign In Register,” (CSMA-75) in accordance with the “Admitting Visitor to a Secured Area of a Customer Service Center” procedure (refer to the FSPA procedure). **END REVISION>>>>>**

EXTERIOR BUILDING SECURITY

1. Have employees open/ close and arrive/depart in pairs.
2. Have shrubbery trimmed and/or cut down around the CSC as needed.
3. Have outside lights replaced and/or added as needed for clear visibility.
4. Ensure dumpsters are not near employee entrances.
5. Install peep holes in all outside solid doors.
6. Ensure surveillance cameras are located in strategic locations.
7. If the CSC still takes deposits to the bank:
    - Disguise bank bags
    - Alternate time and personnel for bank drops
    - Decrease distance between CSC and depository bank.

Return to top of page

CSC MANAGEMENT/DESIGNEE—BEFORE AND AFTER WORK HOURS

CSC management is authorized to work before or after business hours, except on Sundays, to complete non-secure CSC business (such as administrative paper work, review of procedures, review of e-mails, etc.).

- If management/designee must work before or after business hours:
    1. Ensure all secure items and money is locked in the security closet at all times.
    2. Ensure all entrances are locked at all times.
    3. Ensure NO transactions are processed in the system, camera, or other automated systems.
    4. Ensure NO family or friends are allowed inside the CSC.

    NOTE: CSC management is encouraged to limit the time they spend in the CSC before and after business hours to minimize risk to their personal safety. At no time can CSC work be removed from the CSC to be worked on elsewhere.

- If management/designee arrives before work hours:
    1. Park your vehicle in a secure location near the building.
    2. Be aware of your surroundings.
    3. Enter the building quickly.
    4. Disarm the security system.
    5. Lock doors upon entering the building.

6. Ensure the security system is operational and the DVR is recording.

- If management/designee leaves after work hours:
    1. Move your vehicle closer to building before staff leaves.
    2. Ensure all entrances are locked.
    3. Make sure the alarm has been set with the panic buttons activated.
    4. Ensure the door is locked upon exiting.
    5. Be aware of your surroundings.

Return to top of page

CSC MANAGEMENT—PHYSICAL SECURITY

Physical security access includes (but not limited to) the following:

- Arming/disarming the alarm system,
- Holding building keys,
- Having the combination to the safe,
- Having access to the security closet, and/or
- Access to building before and after business hours.

CSC management must limit the number of employees who have access to physical security (see chart below).

Total Number of CSC Employees	Maximum Number of Full-Time CSC Employees with Physical Security Access [1,2]
21 or more	8 Employees
10-20	6 Employees
9 or fewer	4 Employees

[1] District management approval is required if CSC Management determines that additional full-time employees or part-time employees need physical security access.

[2] The number of employees allowed to have physical security access does not include:
- management, mobile designees, work leaders (who will always have access)
- law enforcement personnel.

Management must change the entry code/combination to the security closet anytime access is taken away or access is rotated to other employees. District management, law enforcement and maintenance personnel will **not** have access to the security closet.

> **EXCEPTION:** CSC Management must approve entry if an emergency requires access by non-approved personnel. Management must ensure the security closet code/combination is changed the following day.

ACCESS TO PHYSICAL SECURITY

CSC management at all times must retain the signed, up-to-date reports in the CSC files of CSC employees and all other essential personnel (district office staff, LE, DLQA, TSS, MC, Mobile Employees, maintenance and janitorial services, etc) who have access to any of the following:

- Building alarm system (and the specific code assigned to each employee according to CSCOM-202)
- Building key
- Combination to the safe
- Key and/or combination to the security closet

REQUESTING ACCESS TO PHYSICAL SECURITY

To request physical security access for DMV and non- DMV personnel:

1. Complete the CSC Physical Security Access Report For DMV Personnel (CSMA 32) or the CSC Physical Security Access Report for Non-DMV Personnel (CSMA 33) for the personnel(s) in which physical security access is being requested.
    - The CSMA 32 or CSMA 33 must be completed when there have been changes in physical security access.

- Employees temporarily assigned to a CSC for an extended period of time may be added to the CSMA 32. This must be approved by the District Manager.

2. Forward (email) the access report to the District Manager (or DM designee) for approval and signature.
    - District Manager or designee reviews the report, and if approved, signs the report to authorize increased access.
        - District Manager will retain the original signed report at the District Office, and
        - Email, fax, or mail a photocopy of the signed report to the originating CSC.
3. Retain a copy of the signed access report on file (refer to CSCOM-1101).

    NOTE: The ability to arm/disarm the alarm system, building keys, combination to the safe and doors, and combination to the security closet must be given only to full-time DMV employees. Access must not be granted to P-14 employees in the office without approval from District and CSMA management.
    - Managers must assign a unique code to each employee who is given the ability to arm/disarm the alarm system.

TERMINATING ACCESS TO PHYSICAL SECURITY

1. Change all access locks and/or keypad numbers if an individual who has building access discontinues working in the CSC or if there is a change in the janitorial vendor.
    a. Contact the security company to have transferred or terminated employees removed from the authorized access list and request removal of the employee's access code.

    b. Test the access system to ensure transferred or terminated employees have been removed from the access list.
        - If the employee access code has NOT been removed, CSC management must follow up with the security company to ensure it is deleted. Retest the security system.
        - If the employee access code has been deleted, document that the access code has been deleted (along with the date). Combine all documentation and retain on file at the CSC (refer to CSCOM-1101).
2. Ensure that the keypad to the security closet is changed immediately, for employees who have access to the safe, when they are terminated or transferred.
    - If the CSC is not equipped with a keypad on the security closet door, schedule a locksmith to change the safe combination as soon as possible after the employee's departure.

Return to top of page

ACCESSING LAW ENFORCEMENT DIVISION (LED) OFFICES

1. Access to offices within the CSC that are assigned to Law Enforcement Division (LED) personnel will be limited to LED personnel only, except in the event of an emergency.
2. CSC offices assigned to LED personnel will be secured with either:
    a. a lock and key

    OR

    b. combination lock mechanism
3. The LED agent or, if more than one, the most senior LED agent will provide the CSC Manager with either a copy of the key or the code needed to access the LED office(s) in a sealed envelope; this sealed envelope must be kept in the building safe.
4. In the event of an emergency requiring access to the LED office(s), the Manager or, in the absence of the Manager, his/her designee may retrieve the sealed envelope containing the copy of the key or the code needed to access the LED office(s).
    a. The Manager/designee will lock the LED offices immediately upon resolution of the emergency.
    b. The CSC Manager/designee will notify the appropriate LED Agent as soon as possible and no later than the end of the business day that the LED office key or code had been used.
    c. If circumstances require that the LED office(s) be left open for any extended period:
        i. The Manager or designee will contact the LED Agent immediately. If the Manager/designee cannot reach the LED Agent, he/she will call DMV Enforcement, (804) 367-1678 or (804) 367-1997.
        ii. The Manager/designee will monitor the unlocked LED offices until the LED Agent or another member of LED arrives to do so.

5. If the LED office(s) have been accessed by either the CSC Manager or his/her designee the LED agent will:
   a. Change the door access code and will provide a copy of the new code to the Manger in a sealed envelope **OR**
   b. Retrieve the key from the CSC Manager/designee as soon as possible and, if the LED agent deems it necessary, will contact DMV Facilities Services and have the lock changed. The LED Agent will provide the same or (if the lock was changed) new key copy to the CSC Manager in a sealed envelope.

Return to CSCOM Menu