



RULES OF BEHAVIOR

Logistics Supply Chain Management System Cloud (LSCMS-C)

The following rules of behavior apply to all Department of Homeland Security (DHS) employees, contractors, and authorized users who utilize the Logistics Supply Chain Management System Cloud (LSCMS-C) and its associated IT resources—including workstations, laptops, mobile computing devices (e.g., smartphones, tablets), and cloud-based applications—to access, store, receive, or transmit sensitive information. Compliance with these rules is mandatory to ensure the security, integrity, and confidentiality of the LSCMS-C system and its data.

General Rules

1. **Access Control:** Your access to the LSCMS-C system is limited to the minimum necessary to perform your official duties. If you believe your access level is inappropriate, immediately notify FEMA-TRACC-HQ at FEMA-TRACC-HQ@fema.dhs.gov.
2. **Authentication Credentials:** You must maintain the confidentiality of your authentication credentials (e.g., passwords, PINs). Do not share or disclose your credentials to anyone. DHS personnel will never request your credentials.
3. **Unauthorized Interfaces:** Do not establish unauthorized connections between the LSCMS-C system and other systems, networks, or applications.
4. **Resource Protection:** Safeguard LSCMS-C system resources against waste, loss, abuse, unauthorized use or disclosure, and misappropriation.
5. **System Updates:** Ensure your operating system (OS) and web browser are supported, fully updated, and configured with strong encryption protocols.

System Access

1. **Authorized Access:** Access to the LSCMS-C system is granted solely for official duties. Do not attempt to access systems or data for which you are not authorized.
2. **Classified Information:** Do not process classified information on the LSCMS-C system. Report any inadvertent or unauthorized classified processing to the Information Systems Security Office (ISSO).
3. **PII Restrictions:** Only process the following Personally Identifiable Information (PII) on the LSCMS-C system: names, work emails, department/agency/office affiliation, and work phone numbers.
4. **Password Security:** Choose passwords that are at least 12 characters long, including upper- and lower-case letters, numbers, and special characters. Protect passwords from disclosure and do not share them.
5. **Monitoring and Auditing:** Use of the LSCMS-C system constitutes consent to monitoring and auditing. There is no expectation of privacy when using LSCMS-C.
6. **Idle System Security:** Lock your workstation or enable a password-protected screen saver when idle for short periods. Log off your computer when leaving your work area unattended for extended periods (e.g., overnight).
7. **Authorized Use:** While logged into the LSCMS-C system, conduct only authorized business within the application.

Privacy and Data Handling

1. **Data Disclosure:** Do not retrieve or disclose information from the LSCMS-C system for unauthorized individuals or entities.
2. **Legal Compliance:** Unauthorized access or misuse of information violates the Computer Fraud and Abuse Act and DHS policies.
3. **Data Responsibility:** Users are responsible for ensuring that all data entered into the LSCMS-C system is accurate, secure, and used solely for official government purposes.
4. **Monitoring:** The LSCMS-C system monitors user activity and guarantees no privacy in accordance with government privacy standards.

Incident Reporting

1. **Security Incidents:** Report all security incidents or suspected incidents (e.g., lost passwords, suspicious activity) to your agency's Information System Security Officer (ISSO).
2. **Clarifications:** Contact the LSCMS-C ISSO if you have questions or require clarification regarding these rules.

Acknowledgment Statement

By logging into the LSCMS-C system, you acknowledge and agree to the following:

- Your account carries special privileges, responsibilities, and accountability.
- Sharing account access information, granting unauthorized privileges, or altering user settings without authorization is strictly prohibited.
- Your activities and access will be recorded and periodically monitored. Unauthorized use may result in disciplinary action and referral to supervisory personnel or law enforcement.
- You have read, understood, and agreed to comply with all rules outlined in this document.

Consent

By clicking the LSCMS-C Application Modules you acknowledge that you have read the United States Government Warning Banner and the Rules of Behavior.