RULES OF BEHAVIOR

General Rules of Behavior for Users of DHS Systems and IT Resources that Access, Store, Receive, or Transmit Sensitive Information.

The following rules of behavior apply to all Department of Homeland Security (DHS) employees and support contractors who use DHS systems and IT resources including workstations, laptop computers, and mobile computing devices (including cell phones, smartphones, tablets, removable media such as CDs, DVDs, and both mechanical and solid state portable memory drives) to access, store, receive, or transmit sensitive information.

General Rules

- Your level of access to the LSCMS-C system operated by Manhattan Associates Inc. is limited to ensure your access is no more than necessary to perform your legitimate tasks or assigned duties. If you believe you are being granted access that you should not have, you must immediately notify the FEMA-TRACC-HQ, FEMA-TRACC-HQ@fema.dhs.gov.
- You must maintain the confidentiality of your authentication credentials such as your password. Do not reveal your authentication credentials to anyone; a FEMA TRACC employee should never ask you to reveal them.
- You must not establish any unauthorized interfaces between systems, networks, and applications operated by Manhattan Associates Inc.
- You must safeguard system resources against waste, loss, abuse, unauthorized use or disclosure, and misappropriation.
- You must ensure that you are running a supported and fully updated OS and Web browser and your Web browser is configured with strong encryption.

System Access

- I understand that I am given access only to those systems to which I require access in the performance of my official duties.
- I will not attempt to access systems I am not authorized to access.
- I will not process classified information on LSCMS-C System.
- I will report to the Information Systems Security Office any inadvertent or unapproved classified processing on LSCMS-C System.
- I will not process any PII information on the system besides the following items: Names, Work Emails, Department/Agency/Office Affiliation, and Work Phone numbers.
- I will choose passwords that are at least twelve characters in length and include upper- and lower-case letters, numerals, and special characters. I will protect passwords and access numbers from disclosure. I will not share passwords.
- I understand that the use of Government furnished information systems always constitutes my consent to monitoring and auditing of this use. I understand there is no expectation of privacy when using or storing data on government systems.

- Unless authorized in writing by the System Administrator, I will log off my computer when leaving my work area unattended for extended periods (i.e. overnight). I will use account locking or a password-protected screen saver requiring reentry of my password when my system is idle for short periods of time. When logged in to the operational system Logistics Supply Chain Management System Cloud (LSCMS-C) you must conduct only authorized business within the application.

Privacy

- You must not retrieve information, or in any other way disclose information, for someone who does not have authority to access that information.
- You understand that any person who obtains information from a computer connected to the Internet in violation of the employer's computer-use restrictions is in violation of the Computer Fraud and Abuse Act.
- As user of the system you understand that all data entered is for official government use and holds the responsibility for the data that is entered into the system. Data entered may include Personal Identifiable Information of individuals within your organization; to which you as the user certify that you and the organization will be responsible for maintaining and managing the data.
- You understand that LSCMS-C monitors the system and guarantees no privacy in alignment to Government privacy standards.

Contact Information

- You agree to contact LSCMS-C Information System Security Officer (ISSO) if you do not understand any of these rules.
- You must report all security incidents or suspected incidents (e.g., lost passwords, improper or suspicious acts) to your agency's Information System Security Officer (ISSO).

Acknowledgment Statement

I acknowledge that this account status carries special privileges, responsibilities, and accountability. It is strictly against DHS policy to share account access information with others, allow unauthorized privilege to others, or to change user settings on accounts without proper authorization. I am also aware that my activities and/or access will be recorded by system software and periodically monitored. If this record reveals any unauthorized use, this record may be provided to supervisory personnel and law enforcement officials as evidence. I have read and agree with all the items 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.