FEMA dominKnow Learning Content Management System (LCMS) User Agreement/Rules of Behavior for DHS Users

I, _____, understand, accept, and agree to the following rules of behavior that apply to my access to, and use of information, connected to or in support of the FEMA dominKnow LCMS.

1. DHS GENERAL RULES OF BEHAVIOR

In accordance with the requirements of the Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource, Appendix I" and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, "Guide for Developing Security Plans for Federal Information Systems", DHS established minimum information system rules of behavior for the use of DHS information systems. These Rules of Behavior are consistent with the IT security policy and procedures identified in DHS Directive 140-01, "Information Technology Systems Security;" and the DHS Sensitive Systems Policy Directive 4300A.

The following minimum Rules of Behavior apply to all users of DHS information systems and IT resources (e.g., networks; databases; applications; workstations; laptops; mobile computing devices, including cell phones, smartphones, and tablets; and removable media such as USB drives, CDs, or DVDs), including DHS employees, support contractors, detailees, and all other system users.

These Rules of Behavior apply to users at their primary workplace; telework, satellite, or alternate worksite; and while traveling, domestically or internationally. Information system users that are not subject to Component-specific rule(s) of behavior must comply with this minimum baseline rules of behavior. Any user not in compliance with applicable Rules of Behavior is subject to sanctions that may include verbal or written warning, denial of system access for a specific period of time, reassignment to other duties, criminal or civil prosecution, termination of employment, civil sanctions, or criminal prosecution.

DHS Minimum Baseline Information System Rules of Behavior

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.

Passwords and Other Access Control Measures

- I understand that DHS has a goal of 100% strong identity authentication that will require use of my Personal Identity Verification (PIV) card and Personal Identification Number (PIN).
- In those instances where a password must be used, I will use a password that complies with the appropriate Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) as specified by the system Information Systems Security Officer (ISSO).
- I will protect passwords and PINs from disclosure.

- I will not share passwords or PINs with anyone, including system administrators.
- I will not record passwords or PINs on paper or in electronic form.
- To prevent others from obtaining my password via "shoulder surfing," I will shield my keyboard from view when entering my password or PIN.
- I will promptly change my password or PIN whenever its compromise is known or suspected to have occurred.
- I will ensure that my PIV card is always in my personal possession while at work or performing work-related activities.
- I will promptly report the loss of my PIV card to my supervisor and the DHS Chief Security Office.
- I will not store my PIV card with DHS workstations, laptop computers, or mobile computing devices.
- I will not attempt to bypass access control measures.

Data Protection

- I will use only DHS equipment or DHS authorized and approved services, such as Workplace as a Service (WPaaS), to access DHS systems and information.
- I will protect sensitive information from disclosure to unauthorized persons or groups.
- I will only share information from DHS systems in accordance with all DHS privacy, legal, security, and policy requirements. Should I share personally identifiable information or special protected class data with unauthorized persons or entities, I will immediately report the incident to my Component privacy office in accordance with DHS 4300A Sensitive Systems Handbook Attachment F, "Incident Response."
- I will lock my workstation or laptop computer by removing my PIV card or other secondary authentication device, or I will use a password-protected screensaver, whenever I am away from my work area for a short time.
- I will not access, process, or store classified information on DHS office equipment unless use of the equipment is authorized for classified information of the appropriate level.

Software

- I agree to abide by software copyrights and to comply with the terms of all licenses.
- I will not install on DHS equipment any unauthorized software, including software available for downloading from the Internet, software available on DHS networks, and personally owned software.

Use of Government Furnished Equipment, Internet, and Email

- I understand that I can only use Government systems for official Internet activities and email, with limited personal use allowed. Allowed personal use is described in DHS Directive 142-03, "Electronic Mail Usage and Maintenance" and DHS Directive 262-04, "DHS Web (Internet and Extranet Information)."
- I understand that Government Furnished Equipment (GFE) can only be used in approved geographic location/areas (travel with GFE MUST be approved) and for work purposes.
- I will not use Government systems for access to personal webmail.
- I will not forward government emails to my personal email account.

- I understand that my use of DHS information systems, equipment, and networks, including, but not limited to, Internet and email use may be monitored, and I consent to such monitoring.
- I will not use unauthorized cloud services or peer-to-peer (P2P) file sharing to connect remotely to other systems for the purpose of sharing files. I understand that these services can be a means of spreading viruses over DHS networks and may put sensitive government information at risk. I also understand that DHS Sensitive Systems Policy Directive 4300A prohibits the use of P2P software other than that approved for use by the Department on any DHS-controlled or DHS-operated system.
- I will not provide personal or official DHS information if solicited by email, respond to requests for personal information, verify accounts, security settings, or open any links contained in email unless I know the sender and source have an authorized need to know. I will forward any suspicious or questionable email to DHSSPAM@hq.dhs.gov and take no other action.
- I understand that only content managers designated by the Office of Public Affairs (OPA) may post material to Department and Component intranet sites.
- I understand that personal Internet activities which inhibit the security of DHS information and information systems, or cause degradation of network services are prohibited. Examples of such activity include streaming of audio or video, social networking, peer-to-peer networking, software or music piracy, online gaming, webmail, unauthorized Instant Messaging (IM), and hacking.
- I understand that the use of webmail or other personal email accounts are prohibited on DHS information systems.
- I understand that gambling and the viewing of pornographic or other offensive content is strictly prohibited on DHS furnished equipment and networks.

Teleworking

Employees approved for teleworking at any alternate workplace must adhere to the following additional rules of behavior:

- At my alternate workplace, I will follow security practices that are the same as or equivalent to those required of me at my primary workplace.
- I will physically protect any communications and computing equipment I use for teleworking when they are not in use.
- I will secure and separate official materials from all printed personal documents in my telework location.
- I will protect sensitive data at my alternate workplace. This includes disposing of sensitive information by shredding, burning, pulping, or pulverizing such as to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste. Alternatively, employees can secure materials in a locked file cabinet, locked desk drawer, or a similar locked container and return them to their duty location on recurring intervals for disposal, as outlined in Section K of DHS Management Directive 11042.
- If permitted to print at home, I will take reasonable and appropriate precautions to immediately remove official documents from printers to prevent inadvertent disclosure.

Laptop Computers and Mobile Computing Devices

Use of DHS communications and computing devices is subject to following additional rules of behavior:

- I will use only DHS-approved communications and computing devices to access DHS systems and information.
- I will keep Government Furnished Equipment (GFE) under my physical control at all times, or I will secure it in a suitable locked container under my control.
- I will password-protect any communications and computing devices I use.
- I will take all necessary precautions to protect GFE against loss, theft, damage, abuse, and unauthorized use (e.g., by employing lockable cases and keyboards, locking cables, and removable storage devices). If my equipment or PIV card is lost or stolen, I will immediately report the incident to my supervisor and to the DHS Chief Security Office (onecardssd@hq.dhs.gov).
- When contacted by technical support personnel who request actions on my part, I will verify their authenticity by calling my Component's Help Desk. When I have verified the caller's identity, I will call them as instructed by the Help Desk, and immediately comply with instructions from the technical support personnel to perform update actions, or to make equipment assigned to me available to technical support personnel for updating.
- I will use only DHS-authorized Internet connections or use DHS-approved VPN technology when connecting over the Internet
- I will not make any changes to any GFE system configuration unless I am directed to do so by an authorized DHS system administrator or field service technician.
- I will not program any GFE with sign-on sequences, passwords, or access phone numbers.
- I understand and will comply with the requirement that sensitive information stored on any laptop computer used in a residence or on travel shall be protected using encryption validated in accordance with FIPS 140-2, "Security Requirements for Cryptographic Modules."
- I understand and will comply with the requirement that sensitive information processed, stored, or transmitted on mobile devices, CDs, and previously approved USB thumb drives must be encrypted using approved encryption methods.

Incident Reporting

- I will promptly report IT security incidents (suspected or confirmed) in accordance with DHS CISO procedures for detecting, reporting, and responding to information security incidents in accordance with DHS 4300A Sensitive Systems Handbook Attachment F, "Incident Response."

Accountability

- I understand that I have no expectation of privacy while using any DHS equipment and while using DHS networks or email services.
- I understand that I will be held accountable for all actions performed using my credentials on DHS systems and IT resources.

2. FEMA dominKnow LCMS SPECIFIC RULES OF BEHAVIOR

- I will NOT share my authentication information or access. My dominKnow LCMS account will only be used by me.

- I will NOT attempt to "hack" the FEMA dominKnow LCMS or connected information systems to include subverting data protection schemes, gaining unauthorized access, elevating permissions to data and capabilities that I am not authorized.
- I will NOT attempt to modify content that has not been specifically assigned to me by the LCMS administrator. This includes courses that I am not authorized to modify any assets developed by others (unless granted specific permission).
- I will NOT intentionally modify or delete content that was developed by someone other than myself, even if I have system access to do so, unless I have been granted specific permission from the developer or project team lead.
- I will NOT import/upload copyright protected content to the LCMS unless I have obtained the rights to use the materials with one or more FEMA projects. If license is limited in use, I will record that limitation with the asset in the copyright metadata field.
- I will NOT import/upload personal or inappropriate content to the LCMS.
- I understand that one of the primary capabilities of the LCMS is to share content and that any content that I create or load in the LCMS may be reused and/or modified by others who have access to the system.
- I will immediately report any indication of account intrusion, unexplained degradation or interruption of system or services, illegal or improper possession of content or files, or the actual or possible compromise of data, files, access controls, or systems to the FEMA EMI LCMS Help Desk: FEMA-EMI-LCMS@fema.dhs.gov
- I understand that all content loaded into, developed, modified, and/or comments added to the LCMS will be subject to monitoring.

ACKNOWLEDGEMENT STATEMENT

I acknowledge that I have read, understand, and will comply with the FEMA dominKnow LCMS Rules of Behavior. I understand that failure to comply with the Rules of Behavior could result in one or more of the following actions: verbal or written warning, denial of system access for a specific period of time, reassignment to other duties, criminal or civil prosecution, termination of employment, civil sanctions, or criminal prosecution.

Name of User (printed): _____

User's Email Address: _____

User's Signature: _____

Date: _____