DEPARTMENT OF HOMELAND SECURITY

FEDERAL LAW ENFORCEMENT TRAINING CENTERS

FLETC INFORMATION TECHNOLOGY SYSTEMS AND RESOURCES RULES OF BEHAVIOR AND USE AGREEMENT

Purpose: The purpose of this form is to obtain agreement from users of the Federal Law Enforcement Training Centers' (FLETC) Information Technology (IT) systems and resources. Signing this form signifies understanding and acceptance of applicable policy and legal requirements concerning access to IT systems that transmit, store, or process sensitive FLETC data or information. The following rules of behavior apply to all users, excluding FLETC students, to include FLETC personnel, detailees, guests/visitors, student interns, contractors, and partner organization (PO) personnel when using FLETC IT systems or resources. Additional acceptable personal use guidelines for contractors may be specified in individual contract requirements. These rules do not apply to IT systems or resources owned by FLETC POs. FLETC rules of behavior apply to users at their primary workplace, while teleworking at a satellite site or at home, at any alternative workplaces, and while traveling.

For Official, Approved Use: FLETC IT systems and resources are funded by the U.S. Government to support FLETC's mission. Users are reminded that, when using FLETC IT systems or resources, they are acting in their official capacity, on behalf of FLETC. In accordance with FLETC Directive 140-05, Limited Personal Use of Government Information Technology Resources, users of FLETC IT systems and resources are allowed limited personal use of those systems and resources during non-work time for a reasonable duration and frequency of use that does not adversely affect the performance of official duties or interfere with the mission or operations of FLETC.

Section 1 - General Principles

a. I shall:
   1. adhere to standards of behavior that will reflect credit upon the government while using FLETC IT systems and resources.
   2. only use systems, software, and data for which I have authorization and only for official government business, in accordance with FLETC Directive 140-05.
   3. report IT security events (suspected security incidents), actual incidents, or any incidents of suspected fraud, waste, or misuse of FLETC IT systems or resources to my immediate supervisor, the FLETC IT Service Desk, or the FLETC Cyber Security Operation Center (CSOC).
   4. protect sensitive information from unauthorized disclosure.
   5. comply with FLETC password/personal identification number (PIN) policies and/or specific IT system requirements.
   6. shield the keyboard or similar device from other personnel as I enter passwords/PINs.
   7. promptly change passwords/PINs whenever I suspect or know my password/PIN has been compromised. The compromise or suspected compromise of passwords/PINs must be reported to the FLETC IT Service Desk.
   8. protect my passwords/PINs and other forms of authentication from unauthorized use and disclosure.
   9. change my passwords/PINs when prompted to do so, to include changing default initial passwords/PINs or as directed from authorized IT support or IT security personnel.

b. I shall not:
   1. share my password/PIN with other personnel under any circumstances.
   2. record passwords/PINs on paper or other easily accessed media, or store passwords/PINs with the IT system or resource they access without supplemental security controls such as encryption.
   3. attempt to override system technical, operational, or management controls.
   4. engage in criminal, infamous, dishonest, immoral, notoriously disgraceful, or other conduct prejudicial to the government.

Section 2 - System Access Controls

a. I shall:
   1. invoke a password/PIN protected screensaver and remove my PIV card whenever I leave my system unattended.
   2. notify my supervisor when access to a specific IT system is no longer required to accomplish my assigned duties and responsibilities.
   3. make acceptable alternative provisions for access to information under my control to prevent the sharing of passwords/ PINs with co-workers or other personnel, when I am absent.

b. I shall not:
   1. attempt to access IT systems or resources that I have not been authorized to access.
   2. use my position or access privileges to exploit system controls or access information for any reason other than in the performance of my official duties.
   3. attempt to bypass access control measures or to exceed my system specific access privileges.
   4. allow other personnel to use FLETC IT systems or resources with my system access credentials (e.g., user ID, password, PIV card) at any time.

Section 3 - Information Protection

a. I shall:
   1. mark storage media or removable media (e.g., diskettes, thumb drives, CPUs with fixed hard drives, compact disks (CDs), etc.) with the appropriate sensitivity caveat (e.g., For Official Use Only, Law Enforcement Sensitive, Controlled Unclassified Information) of the highest level of data sensitivity ever contained on the media.
   2. secure storage media, removable media, and hardcopy output in accordance with the highest level of data sensitivity ever contained on the media (e.g., locked office, file drawer).
   3. dispose of storage media and hardcopy output containing sensitive information using FLETC approved sanitization and destruction methods, tools, and procedures (e.g., overwriting disks, shredding, burning, degaussing media, etc.).

b. I shall not:
   1. share or disclose sensitive information except as authorized and with formal agreements that ensure third-parties will adequately protect it.
   2. store sensitive information in public folders or other insecure physical or electronic storage locations.
   3. knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information.
   4. use sensitive information for anything other than the purpose for which it has been authorized.

Section 4 - Hardware

a. I shall only use FLETC owned or approved IT systems or resources to accomplish my official duties with limited personal use in accordance with DHS and FLETC directives, policies, manuals, and instructions. Specific direction is provided in FLETC Directive 140-05, and DHS Management Directive 4600.1, Personal Use of Government Office Equipment.

b. I shall not:
   1. remove or relocate IT resources from FLETC premises unless authorized in accordance with FLETC IT and Property Management policies.
   2. install, connect, or remove FLETC IT systems or resources (e.g., hardware, devices, components, workstations, laptops), without prior approval from the Chief Information Officer (CIO) Directorate.

c. I understand:
   1. that use of FLETC IT systems, resources, or office equipment may be monitored, and I consent to this monitoring.
   2. that the viewing, storage, sharing, or use of pornographic or other offensive content is strictly prohibited on FLETC owned or approved IT systems and resources.

Section 5 - Software and Applications

a. I shall abide by software copyrights and comply with the terms of license agreements.

b. I shall not:
   1. duplicate or remove copyrighted software (except for backup purposes and according to manufacturer's guidance) from FLETC owned or approved IT systems or resources without the expressed written permission of the CIO Directorate.
   2. use file sharing applications/software, known as peer-to-peer (P2P), to connect remotely to other systems, resources, or devices for the purpose of, but not limited to file sharing.

c. I understand that I may be personally liable for any software copyright violations associated with government owned software.

Section 6 - Use of Internet and Email Resources

a. I shall only use FLETC IT resources for official business related Internet activities and email, with limited personal use as allowed in FLETC Directive 140-05.

b. I shall not:
   1. view Internet sites containing malicious, hostile, threatening, abusive, vulgar, defamatory, profane, or racially, sexually, or ethnically objectionable content (e.g., text, graphics, music, etc.).
   2. send email that contains malicious, hostile, threatening, abusive, vulgar, defamatory, profane, or racially, sexually, or ethnically objectionable content.
   3. post information that contains malicious, hostile, threatening, abusive, vulgar, defamatory, profane, or racially, sexually, or ethnically objectionable content to Internet sites, chat rooms, message boards, or other open forum discussions using FLETC IT systems or resources.
   4. use FLETC or government provided Internet services or email for outside fund-raising, lobbying, commercial business, or other prohibited activities.
   5. provide personally identifiable information (PII), official FLETC information, or other sensitive information if solicited for such information by email. If I receive an email message from any source requesting PII or asking to verify IT system user account information or security settings, I must validate the source email, seek supervisory or security direction before responding, and report the security event to the FLETC CSOC.
   6. use Internet site capabilities on FLETC provided or approved IT systems or resources to bypass security controls or cause degradation of network services.
   7. email sensitive information (e.g., For Official Use Only, Law Enforcement Sensitive, and Controlled Unclassified Information) to personal email accounts under any circumstances.

8. email sensitive information (e.g., For Official Use Only, Law Enforcement Sensitive, and Controlled Unclassified Information) to non-DHS email addresses without securing the information using supplemental security controls such as encryption.
9. setup auto-forwarding of email to any address outside of the .gov and .mil domain.

c. I understand that my Internet and email use and activities may be monitored, and I consent to such monitoring.

Section 7 - Use of Chat, Instant Messaging, and Cellular Text Messaging Systems

a. I understand that DHS policy prohibits the use of chat, instant messaging, and cellular text messaging systems to formally transact agency business or to document the activities of the organization. However, DHS also recognizes that during exigent circumstances, staff may need to conduct official agency business using these systems.

b. If required to conduct official agency business using these systems during exigent circumstances, I shall:
   1. comply with DHS records management policies.
   2. take steps to document the official agency business that was conducted using these systems through other means (i.e., email, memo for record).

c. I shall not use these systems to formally transact agency business or document the activities of the organization during normal circumstances.

Section 8 - Telephone Equipment and Services

a. I shall:
   1. protect my telephone voice mail system password/PIN in accordance with FLETC password/PIN policies and specific IT system requirements.
   2. avoid or limit the use of standard telephone equipment for conversations involving highly sensitive information.

b. I shall not:
   1. use FLETC telephone equipment, facsimile (FAX) machines, or other forms of telephone services for personal long distance calls unless a personally owned credit calling card or collect call is used. Limited personal use is allowed as described in FLETC Directive 140-05.
   2. use standard telephone equipment for conversations involving classified information. Designated secure telephones are available on FLETC facilities for classified discussions.

Section 9 - Remote Access and Telecommuting

a. I shall:
   1. follow security policies when teleworking, traveling, or working from other off-site, remote, or non-FLETC facilities locations.
   2. protect sensitive information used at remote sites in accordance with FLETC directives, which includes, but is not limited to, properly disposing of information and protecting information from unauthorized disclosure when processed on non-FLETC computers.
   3. only remotely access FLETC owned or approved IT systems using approved remote access devices, software, and services.
   4. protect remote access support information such as Internet access addresses, and access credentials such as passwords from unauthorized disclosure.

b. Employees approved for teleworking at any alternate workplace must adhere to the following additional rules of behavior: I shall:
   1. follow security practices, at my alternate workplace, that are the same as or equivalent to those required of me at my primary workplace.
   2. physically protect any equipment (e.g., desktops, laptops, printers, or personal electronic devices) I use for teleworking when they are not in use.
   3. protect sensitive data at my alternate workplace. This includes disposing of sensitive information by shredding or other approved destruction capability.

Section 10 - Mobile IT Resources

a. I shall:
   1. keep laptops and other forms of FLETC mobile IT resources (e.g., cell phones, smartphones, tablets) containing sensitive information under my physical control or ensure the resources are appropriately protected (e.g., locked in a controlled area cabinet, building, or space) against loss, theft, damage, abuse, or unauthorized access when unattended.
   2. ensure anti-virus software, firewalls, and software patches are installed and kept current on laptops and other mobile IT resources, following CIO Directorate processes and procedures.
   3. encrypt sensitive information stored on laptops and other mobile IT resources using FLETC approved encryption capabilities when available.
   4. password-protect any FLETC provided IT mobile resources I have been issued or use.
   5. use any camera, video, or audio recording capabilities on mobile IT resources for official authorized purposes only, to include limited personal use in accordance with FLETC Directive 140-05.

6. report lost, misplaced, or stolen FLETC owned or approved IT resources to local law enforcement, the FLETC IT Service Desk, my supervisor, and the Office of Security and Professional Responsibility, as appropriate.
7. avoid discussing highly sensitive information using mobile IT resources, as these resources are subject to electronic intercept.
8. disable mobile IT resource features that automatically capture and store information without my knowledge, such as embedding location information in pictures taken with the device, if available and not automatically disabled.

b. I shall not:
1. connect personally owned or non-FLETC owned or sponsored laptops or other mobile IT resources to FLETC IT systems or resources unless specifically authorized.
2. connect any personally owned IT resource (e.g., laptop) to a FLETC/government issued mobile IT resource to gain access to Internet services.
3. make any changes to a laptop's or other mobile IT resource's system configuration unless specifically approved through the FLETC IT Service Desk, to include, but not limited to enabling wireless ports and capabilities.
4. use any non-FLETC owned or approved laptop or other mobile IT resource to store sensitive information without prior approval from the CIO Directorate.
5. use any mobile IT resource, FLETC provided, contractor provided, or personally owned, while operating a government vehicle.
6. use standard mobile IT resources to process, store, or transmit conversations involving classified information. Designated mobile IT resources are available on FLETC facilities for classified discussions.

c. I understand:
1. that I am authorized to connect a FLETC/government issued mobile IT resource to a FLETC/government issued IT resource (e.g., laptop) to gain access to Internet services and access to FLETC IT systems or resources. This concept is known as tethering.
2. that certain foreign governments routinely target government officials for electronic intercept and other intelligence gathering activities.

Section 11 - Classified National Security Information Processing

a. I shall report any suspected security violations involving the inappropriate use of classified national security information on an IT resource to the FLETC CSOC.

b. I shall not:
1. process, store, or transmit, classified national security information on any FLETC IT system or storage media not specifically approved and marked for classified processing and storage.
2. process, store, or transmit classified national security information on any personally owned IT systems, mobile IT resources, or storage media.

c. I understand that:
1. in the event of a spillage of classified national security information to an unclassified IT system or network or to a personally owned IT device, the personally owned IT device and removable media, used during the spillage, will be surrendered to FLETC, may require physical destruction, and that I may not be compensated for the loss. Should I cause the event to occur, I will not be compensated for the loss of personally owned IT. I further understand that I, or the owner of the IT, may not be compensated for the lack of access or use of the IT or for the loss of data on the IT.
2. should I use personally owned IT devices to access government IT systems or resources; I accept all risks associated with such use to include the loss of the personally owned IT device and all data stored on the personally owned IT device.
3. any IT system or storage media used to process classified national security information is considered a classified resource and must be appropriately marked, handled, and stored as a classified resource.
4. the mishandling of classified national security information may affect my ability to obtain or maintain a security clearance and could result in civil and criminal penalties.

Acknowledgment Statement

I understand that I have no expectation of privacy while using any FLETC IT resources to include Internet access and email. I further understand that my access and use is subject to monitoring, recording, and auditing for any lawful government purpose.

I acknowledge that I have read and understand these rules of behavior. I understand that non-compliance with these rules may result in disciplinary action, as well as civil and criminal penalties.

Name, Signature, & Date:	
Organization:	

Submit by Email | Print Form