

Rules of Behavior and Acceptable Use Standards for Air Force Information Technology

The following statements reflect mandatory behavioral norms and standards of acceptable use of Air Force Information Technology. By signing below, you indicate both your understanding of these standards, and your agreement to act in accordance with them as a condition of your service with or access within the Air Force. Air Force Instruction 17-130, *Cybersecurity Program Management*, applies.

1. I WILL adhere to and actively support all legal, regulatory, and command requirements.

- a. I understand that Air Force Information Technology is to be used primarily for Official/ Government Business, and that limited personal use must be of reasonable duration and frequency that have been approved by the supervisors and do not adversely affect performance of official duties, overburden systems or reflect adversely on the Air Force or the DoD.
- b. I will not use my access to government information or resources for private gain.
- c. I waive my expectation of privacy in my Air Force electronic communications. This is not a waiver of my rights to attorney-client privilege, medical information privacy, or the privacy afforded communications with religious officials/chaplains.
- d. I will observe all software license agreements and Federal copyright laws.
- e. I will encrypt sign and any message containing For Official Use Only or Personally Identifiable Information.
- f. I will promptly report all security incidents in accordance with Air Force policy.

2. I WILL use the system in a manner that protects information confidentiality, integrity and/or availability.

- a. I will not store or process classified information on any system not approved for classified processing.
- b. I will protect my Common Access Card token from loss, compromise, or premature destruction. I will not share my token/credentials with anyone, use another person's token/credentials, or use a computer or terminal on behalf of another person.
- c. I will protect my passwords/Personal Identification Numbers from disclosure: I will not post or write these down in my work space.
- d. I will lock or log-off my computer or terminal any time I walk away.
- e. I understand that my password/Personal Identification Numbers must adhere to current Air Force standards for length, key-space, and aging requirements.
- f. I will not disclose any non-public Air Force or DoD information to unauthorized individuals.
- g. I understand that everything done using my Common Access Card/password/Personal Identification Number will be regarded as having been done by me.
- h. I will employ anti-malware software and update it as required; I will immediately notify my Information System Security Officer if I believe Air Force Information Technology assets entrusted to me have been compromised; I will take immediate measures to limit damage.

3. I WILL protect the physical integrity of computing resources entrusted to my custody or use.

- a. I will protect Air Force Information Technology from hazards such as liquids, food, smoke, staples, paper clips, etc.
- b. I will protect Air Force Information Technology from tampering, theft or loss; I will take particular care to protect any portable devices and media entrusted to me, such as laptops, cell phones, tablets, disks, and other portable electronic storage media.
- c. I will protect Air Force Information Technology storage media from exposure to physical, electrical, and environmental hazards. I will ensure that media is secured when not in use based on the sensitivity of the information contained, and practice proper labeling procedures.
- d. I will not allow anyone to enter DoD or Air Force facilities without proper authorization.

e. I will not install, relocate, modify, or remove any Air Force Information Technology without proper approval.

4. I WILL NOT attempt to exceed my authorized privileges.

- a. I will not access, research, or change any account, file, record, or application not required to perform my job.
- b. I will not modify the operating system configuration on Air Force Information Technology without proper approval.
- c. I will not move equipment, add or exchange system components without authorization by the appropriate approval of my local systems manager or local hardware custodial personnel.
- d. I will not use, or connect to, non-official hardware, software or networks for official business without proper approval and without the use of authorized mobile device network encryption.

5. I WILL NOT use systems in a way that brings discredit on Air Force users or the Air Force, or degrade Air Force missions.

- a. I will practice operational security in accordance with guidance contained in Air Force Instruction 10-701, *Operations Security*.
- b. I will not receive or send inappropriate material using my official email or Internet accounts.
- c. I will not originate or forward chain letters, hoaxes, or items that advocate or support a political, moral or philosophical agenda.
- d. I understand that pornography, sexually explicit or sexually oriented material, nudity, hate speech or ridicule of others on the bases of protected class (e.g., race, creed, religion, color, age, sex, disability, national origin), gambling, illegal weapons, militant, extremist, or terrorist activities will not be tolerated.
- e. I will not connect or remove any form of removable media without proper approval.

6. I WILL NOT waste system and network resources.

- a. I will not make excessive use of my official computer to engage with social media for personal purposes (e.g., Facebook, Twitter, Instagram, Snapchat, etc.)
- b. I will not make excessive use of my official computer for shopping, or to view full-motion video from non-official sources (e.g., YouTube, online multiplayer video games, etc.)
- c. I will not autoforward e-mail from my official account to a personal e-mail account.

Signature

Date

Printed name (Last, First, MI)

Rank/Position