

**DISA DECC SATX VISITOR STATEMENT OF INFORMATION SYSTEM USE AND  
ACKNOWLEDGEMENT OF SECURITY POLICIES**

I will use DISA Information Systems for official use and authorized purposes only in accordance with DoD 5500.7-R, Joint Ethics Regulation. I will not introduce or process data which the Information System has not been specifically authorized to handle. I understand that all information processed on DISA controlled Information Systems is subject to monitoring. I may also be held both criminally and financially responsible for any damages that may occur to the network, systems, other electrical and non-electrical equipment, or computing devices, if my actions are determined to be deliberate, willful, or malicious.

I understand that I am responsible for all actions taken under my account. I will not attempt to “hack” the network, any connected Information Systems, or gain access to data which I am not authorized.

I understand my responsibility to appropriately protect and label all output generated under my account to include printed materials, floppy disks, and downloaded hard disk files.

I understand I must have the requisite security clearance and documented authorization of my need-to-know before accessing DISA/DOD information and Information Systems.

I understand it is my responsibility to ensure Privacy Act, and other protected personal information (such as personally identifiable information) is protected while it is being processed or accessed in computer environments outside the DISA physical data processing installations requiring access to DISA information and Information Systems (such as remote job entry stations, terminal stations, minicomputers, microprocessors, and similar activities). I know I must ensure appropriate protection of personal and sensitive data.

I understand that my visitor badge will be displayed, with picture showing, above the waist, and only while inside DISA DECC SATX. When departing the premises, I will return my badge and key fob to the Security Desk.

I understand tailgating or piggybacking through doors in the DISA DECC SATX is not permitted. Any misuse of my access or allowing any other person to misuse my access is a felony.

I understand that I am expected to sign in and out as a visitor on the visitor log at each collateral room. If I have been authorized a key fob, I will write key fob in the escort portion of the log.

I understand that if I am escorting personnel I will be responsible for each person and ensure they sign in and out of the visitor log books daily.

**Initial:** \_\_\_\_\_ **Date:** \_\_\_\_\_

I understand that any unauthorized devices that are connected to the network or Information System without prior approval will be confiscated by the Information Assurance Manager (IAM) or senior IA Technical Level representative. This device or media will become property of DISA DECC SATX.

I will immediately report any indication of computer network intrusion, unexplained degradation, or interruption of network services, or actual or possible compromise of data or file access controls to the appropriate Information Assurance Management or senior IA Technical Level representatives.

I understand that it is my responsibility to ensure that my work area is clean and tidy upon completion of work.

I understand that media and software cannot be left unsecured at any time. I will ensure that any media and software used during my visit is secured upon completion of use.

I understand that I am prohibited from the following:

- Introducing classified information into an unclassified system or environment.
- Connecting an unclassified device to a classified network.
- Violating the established security, release, and protection policies for information identified as Classified, Proprietary, Controlled Unclassified Information (CUI), For Official Use Only (FOUO), or Privacy Act-protected during the information handling states of storage, process, distribution or transmittal of such information.
- Obtaining, installing, copying, pasting, transferring, or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement. This includes peer-to-peer file sharing software or games.
- Installing any unauthorized software (license software, games, entertainment software) or hardware (e.g., sniffers).
- Connecting unauthorized devices to the network or Information Systems.

I will not install, modify, or remove any hardware or software (i.e. freeware, shareware, security tools, etc.) without written permission and approval from the Information Assurance Manager (IAM) or senior IA Technical Level representative.

I will not remove or destroy system audit, security, event or any other logs without prior approval from the IAM or senior IA Technical Level representative.

I will not introduce any unauthorized code, Trojan, horse programs, malicious code, or viruses into DISA Information Systems or networks.

I will not allow user access to the network or any other connected system that is not cleared without prior approval or specific guidance of the IA Management.

I will not use any DISA controlled Information Systems to violate software copyright by making illegal copies of software.

**Initial:** \_\_\_\_\_ **Date:** \_\_\_\_\_

I understand that failure to comply with the requirements of this agreement will be reported and investigated. The results of the investigation may result in one or all of the following actions:

- Immediate revocation of facility access
- Confiscation of equipment or devices
- Revocation of Security Clearance
- Uniform Code of Military Justice and/or criminal prosecution
- Disciplinary action, reassignment, discharge, or loss of employment.

**I have read, understood, and will comply with the requirements set forth in this above agreement.**

**Print Name:** \_\_\_\_\_

**Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_