UNCLASSIFIED/FOUO		
KVM (Keyboard Video Mouse) USER AGREEMENT		
PRIVACY ACT STATEMENT		
AUTHORITY: 5 U.S.C. 301; 10 U.S.C. 131. PRINCIPAL PURPOSE(S): Identifies the user of the KVM device as receiving usage and security awareness training governing use of the device and agreeing to use the device in accordance with security policies. The information is used for inventory control of the device and to verify compliance with DoD requirements regarding accountability security requirements IAW Sharing Peripherals Across the Network Security Technical Implementation Guide (SPAN STIG) 3.1 ROUTINE USE(S): None. DISCLOSURE: Voluntary; however, failure to provide the requested information will result in denial to operate or use of the KVM.		
PART I - PERSONAL INFORMATION		
1. LAST NAME	2. FIRST NAME	3. MIDDLE INITIAL
4. RANK/RATE	5. ORGANIZATION	6. DEPARTMENT/DIVISION
7. BUILDING NUMBER	8. ROOM NUMBER	9. WORK TELEPHONE NUMBER
10. E-MAIL ADDRESS		
PART II - USER AGREEMENT – Standard Mandatory and Consent Provision		

User Will:

- Ensure that the switches are approved before installing
- Ensure that the systems are installed correctly and meet all TEMPEST standards
- Ensure the desktop banners, backgrounds, and screen locks have the proper classification banner
- Protect the system and KVM in your area
- Report any spillage of classified information to your IAO or the IAM
- Safeguard and report any unexpected or unrecognized computer output, including both displayed or printed products
- Use different passwords on each system connected through a KVM
- Ensure that the classification level is displayed by each systems screen lock and that the password is required to regain entry to the system
- Ensure that the systems screen lock is invoked if the system is left unattended of if there is a 15-minute period of inactivity for each system
- Be responsible for marking/labeling magnetic media

Administrative Procedures: Users are required to follow the procedures below when using KVM switches:

1. Logon onto an IS.
   a. Identify the classification of the IS currently selected.
   b. Use the login and passwords appropriate for that IS.
   c. Verify the classification of the present IS by checking the classification label/banner.
   d. Begin processing.

2. Switching between ISs.
   a. Screen lock the IS you are currently using if the IS supports this capability.
   b. Select the desired IS with the switch.
   c. Enter the user identifier and password to deactivate the screen lock on the newly selected IS.
   d. Verify the classification of the present IS by checking the classification label/banner.
   e. Begin processing.

Physical Security Controls:

KVM switches are normally unclassified devices; however, it must be protected in a manner suitable for the IS with the highest classification to which it is connected. For example, if the switch is connected to a classified system and an unclassified system, then it will be protected in the same manner as the classified system. Physical access to the KVM switch must also be restricted to individuals that are allowed physical access to all ISs attached to the system.

Labels:

All IS components must be labeled, including all switch positions. They must be clearly marked with the appropriate classification labels.

Desktop Backgrounds:

To avoid inadvertent compromises, systems joined by multi-position switches will utilize desktop backgrounds that display classification banners at the top or bottom. The classification banner will state the overall classification of the system in large bold type, and the banner background will be in a solid color that matches the classification (Secret - red, Confidential - blue, Unclassified - green).

When systems have a similar classification level, but require separation for releasability or other constraints, use of unique colors for the different systems is permissible.

Screen Locks:

Screen lock applications must display the highest classification of the system on which the system is currently logged into and shall implement a lockout feature to re-authenticate the user.

Smart Keys:

Systems using KVM switches must not employ “smart” or memory enhanced/data retaining keyboards, monitors or mice. These types of interfaces provide memory retention that creates a risk of data transfer between systems of different classifications. This includes keyboards with smart card readers, Universal Serial Bus (USB) ports, and removable media drives.

Hot Key Capability:

If the switch has configurable features, the configuration must be protected from modification by the user with a DOD compliant password.

Switches featuring the ability to automatically toggle between Information Systems (IS) must have this feature disabled. The only “hot key” feature permitted to be enabled is the menu feature that allows the user to select the IS to be used from a displayed menu.

Scanning Capability:

Switches with the ability to automatically scan and switch to different CPUs are prohibited.

Wireless or Infrared Technology:

Systems using KVM switches must not use keyboards or mice with wireless or infrared technology.

Connectors:

The use of switches to share peripherals other than the keyboard, video/monitor, and mouse by connecting peripherals to ISs of different classification levels is prohibited. All switches that are attached to ISs of different classifications will have this feature disabled. Regardless of whether it can be disabled, no peripheral devices other than the keyboard, video/monitor, or mouse will be connected to the KVM switch.

Connectors used for this feature will be blocked with tamper resistant seals. Additionally, all unused connectors for ISs will be blocked with tamper resistant seals. All cable connections will be marked with tamper resistant seals that allow visual confirmation that the configuration of the cable has not been modified.

Unique Password:

At a minimum, users must ensure that they use different/unique passwords for each system connected through a switch. System administrators should employ different logon USERIDs to help users further distinguish between the systems.

Training:

Periodic training is required to ensure that users are trained and in compliance with the requirements associated with the introduction and use of KVM switches.

FOR REPORTING PROBLEMS OR TO ASK QUESTIONS, CONTACT NCTS-ME Enterprise Service Desk (ESD): 439-6287

By signing this document, I acknowledge that I have read and understood my duties and responsibilities in relation to the use, operation, and information security requirements of the KVM switch.

12. SIGNATURE OF USER	13. DATE SIGNED (YYYYMMDD)

UNCLASSIFIED/FOUO