Acceptable Use Agreement / Policy

By signing this document, You acknowledge and consent to the following rules of conduct and policies when accessing the United States Military Academy's (USMA) networks, to include the Internet:

1. In Accordance With (IAW) DoD CIO's Standard Consent Policy Memorandum dated 9 May 2008, "You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations, and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential."

2. USMA authorizes the connection of non-government furnished equipment (GFE) (e.g., personally-owned/Bring your Own Device (BYOD) systems, research partner's devices) to the USMA network(s) (e.g., West Point Research and Education Network (WREN) and others as fielded) on several conditions: device registration with USMA; devices 'comply to connect' to the network (e.g., up-to-date operating system, up-to-date anti-virus); when using device(s) to access organizational data (e.g., Exchange, SharePoint) use of USMA mobile device management (MDM) capabilities (e.g., Intune); formal exceptions to Army policies regarding non-GFE equipment on USG networks. a. When accessing secured U.S. Government Information Systems from your non-GFE device, you freely and voluntarily consent to applicable site conditions and government monitoring and collection by government authorities, consistent with the boundaries of the DOD Banner. USMA will respect the privacy of your personal device and will only request access to the device by technicians to implement security controls or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings. This differs from policy for government-provided equipment/services, where government employees do not have the right, nor should they have the expectation, of privacy while using government equipment or services. b. Owners/operators acknowledge that government-provided third-party software (e.g., Company Portal, Microsoft Defender™) may decrease the available memory and/or storage on the device(s) and that USMA is not responsible for any loss or theft of, damage to, or failure in the device that may result from use of third-party software and/or use of the device on the WREN.

c. Owners/operators understand that contacting vendors for trouble-shooting and support of third-party software is their own responsibly, with only multi-factor authentication reset support available from USMA—USMA's Gold Coats will continue to provide hardware and USMA-Enterprise software support to cadets for cadets' bulk-purchased but personally owned laptops.

d. Owners/operators understand use of their devices for USMA or other official activities may result in increases to their personal monthly service plan cost(s). Owners/operators further understand USMA will not reimburse for any such increases in costs.

e. Owners/operators agree that upon ceasing formal official affiliation, USMA requires the owners/operators to remove USMA provided applications, application keys, operating systems, and USG data. They also agree that USMA may conduct such removal remotely if the need arises.
f. Owners/operators agree that when they cease formal official affiliation with USMA (e.g., cadet's graduation or separation from USMA, employee termination/departure, Soldiers' permanent change of station/retirement/separation, research project conclusion) they will lose access to USMA-provided operating system(s) and application(s) licenses and USMA provided storage.

3. Authorized network activity: USMA CIO/G6 created and maintained IS images, and the executables in those images, have default authorization for use. The USMA Acceptable Use Addendum has additional information USMA leaders and users must be aware of given USMA's unique mission and environment.
4. The list of unauthorized network activity is long and partially enumerated in United States Corps of Cadets (USCC) and USMA Regulations and policies, AR 25-1, AR 25-2, the Joint Ethics Regulation, and the acceptable use addendum. The list of unauthorized activity is infeasible to completely enumerate. Rules of thumb include do nothing that is illegal, immoral, or unethical; do not inflict risk on the academy that exceeds your level of authority to assume risk.
5. You acknowledge that in the event of a classified information spillage, the system(s) with the classified data are subject to seizure IAW due process requirements. USMA will, as feasible, forensically wipe the classified data and return, as feasible, the sanitized device(s). USMA, at its discretion, may provide a temporary GFE device to replace a GFE device or a cadet's primary laptop. USMA will not provide a temporary device for non-GFE devices. USMA will not reimburse the owners/operators for the loss of the device should return of a personal device be infeasible to mitigate the risks of the classified data spillage. USMA CIO/G6 activities to mitigate against information spillage will occur in coordination with appropriate law enforcement activities. 6. You acknowledge that USMA may obtain an over-the-network copy of a user's disk(s) from GFE, to include personal data, at any time, during an official investigation into conduct on this network, without obtaining additional permission.
7. You acknowledge that you are responsible for understanding and abiding with what USMA has authorized (and not authorized) for usage/behavior (See also USMA Regulation 25-2 Cybersecurity and its supporting implementing policy documents at USMA G5's Document Library).
8. You acknowledge that you will abide by USMA or DoD-specified controls when storing, processing, or transmitting controlled unclassified Information (CUI) (e.g., others' Personally Identifiable Information, For Official Use Only (FOUO), Privacy Act protected data). Owners/operators agree that should they lose any device that contains CUI they will report the loss to USMA's Cybersecurity (cyber@westpoint.edu) for reporting to HQDA and mitigating the loss of controlled access to the CUI (e.g., remote removal of the CUI data). USMA reserves the prerogative to remotely wipe lost GFE. Users may request CIO/G6 remotely wipe or remotely disable their lost personal device.
9. You acknowledge that violations of this AUP, West Point, Army, DoD, or Joint regulations/policies, or USMA addendums, may result in consequences including, but not limited to loss of network access; loss of administrative privileges on government-managed system(s); loss of other network provided service(s); civilian or military administrative action; civilian or military criminal action.

I have read the statement above and will comply accordingly.

_____	_____	_____
Printed Name/xNumber	Signature	Date