DEPARTMENT OF THE NAVY
UNITED STATES NAVAL ACADEMY
121 BLAKE ROAD
ANNAPOLIS, MARYLAND 21402-1300

USNAINST 5230.1D
ITSD
17 Jun 2026

USNA INSTRUCTION 5230.1D

From: Superintendent, U.S. Naval Academy

Subj: INFORMATION TECHNOLOGY AND CYBERSECURITY POLICY AND STANDARDS

Ref:
(a) DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks," 16 Feb 2024
(b) DoDD 5230.09, "Clearance of DoD Information for Public Release," 25 Jan 2019
(c) DoDD 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," 27 Jul 2017
(d) "DoDCIO Policy on Use of Department of Defense Information Systems Standard Consent Banner and User Agreement," 9 May 2008
(e) SECNAV M-5210.1, "Department of the Navy Records Management Program," Sep 2019
(f) SECNAVINST 5239.25, "Department of the Navy Cyberspace Workforce Qualification and Management Program," 10 Oct 2023
(g) "United States Navy Higher Education Network Cybersecurity Concept of Operations (CONOPS)," 23 Feb 2020
(h) USNAINST 5211.3E, "US Naval Academy Privacy Program," 15 May 2023
(i) USNAINST 5231.1D, "Information Technology Life Cycle Management Policy," 19 Jan 2022
(j) USNAINST 5510.8C, "Information and Personnel Security Manual," 13 Feb 2024
(k) USNAINST 7320.10, "USNA Management of Personal Property," 06 Aug 2014
(l) USNAINST 8510.01, "Cybersecurity Risk Management," 20 Jan 2016
(m) USNACIO M-8510.01, "Risk Management Policy and Standards Manual," 01 Jan 2017

Encl:
(1) Information Technology and Cybersecurity Policy and Standards
(2) Providing IT Assets, Services, and Support to Exchange Students

1. Purpose. To establish information technology (IT) and cybersecurity policy and standards for the U.S. Naval Academy (USNA) per references (a) through (k).

2. Cancellation. USNAINST 5230.1C.

3. Scope and Applicability. All provisions of this instruction apply to all organizations and personnel using any USNA IT resource, including mission and non-mission network infrastructure, hardware, software, and both on-premises and cloud services.

4. Background.

a. The institutional IT policies and standards provide the structure and discipline necessary

to support productivity and effective operations. These policies and standards enable the delivery of cost-effective services while maintaining currency with evolving technology. Well-defined policy is particularly critical in an environment characterized by limited budgets, reduced IT support staff, increasing demand for technology, training requirements, shortened product life cycles, the urgency of immediate service, reliance on IT for mission support, and constraints imposed by external authorities. This framework establishes the foundation for prudent management of IT resources and provides a structured methodology for selecting methodologies and making informed, mission-aligned decisions.

b. The USNA embraces an information-engineered IT environment. Information engineering refers to the seamless integration of technologies to support teaching, learning, training, research, management, communication, and decision-making. This approach focuses on transforming raw data into accurate and actionable information, minimizing complexity for end users, and enabling productivity across all skill levels.

c. The USNA information environment is committed to the adoption and implementation of Zero Trust Architecture (ZTA). This principle assumes no implicit trust is granted to assets or user accounts based solely on their physical or network location. All access to data and resources must be continuously verified based on user identity, device health, and other contextual attributes. Future IT modernization, system design, and security controls must be implemented to support a ZTA model, ensuring that the environment remains resilient against modern cyber threats.

d. IT solutions within the environment must be affordable, achievable, flexible, scalable, interoperable, and secure. All systems and services must be designed to support long-term sustainment, growth and future modernization in accordance with enterprise architecture principles and the Risk Management Framework (RMF). This ensures that USNA remains compliant with the standards set for in references (a) and (k) while protecting the integrity of the collective mission.

(1) Affordable means that available financial resources support the acquisition, operation, maintenance, modernization, and eventual replacement of technology.

(2) Achievable means that existing staffing and skill sets can support acquisition, integration, and ongoing operations throughout the system life cycle.

(3) Flexible means that technology supports multiple mission-related functions and use cases.

(4) Scalable means that technology can accommodate varying levels of demand without significant redesign or performance degradation.

(5) Interoperable means that systems integrate and exchange information effectively with other authorized enterprise systems and services and includes a defined path to support future growth and modernization.

(6) Secure means that policies, technical controls, and supporting infrastructure are implemented to manage risks to the confidentiality, integrity, and availability of information and services in accordance with RMF requirements.

5. Responsibilities.

a. Chief Information Officer (CIO). The CIO (Deputy Director for IT) is the primary

authority for the strategic management and oversight of the USNA Academic and Professionally Accredited Educational Enterprise Enclave (AEEE). The CIO must ensure institutional compliance with all applicable federal, DoW and DON IT policies. The CIO is responsible for promulgating the overarching policies and standards required to implement this instruction and must conduct an annual review of this policy annually to ensure continued alignment with evolving federal directives.

b. Command Security Manager (CSM). The CSM serves as the functional lead for personnel security and institutional trust. To maintain the integrity of the AEEE, the CSM must conduct annual command-wide audits of all positions to validate mission-based requirements for network access and privileged entitlements in accordance with reference (a). This process confirms that all system access is supported by background investigations meeting federal and DoW standards. The CSM must collaborate with the administrative authorities to ensure IT access remains commensurate with current position descriptions and investigative status, and must coordinate with the Information Systems Security Manager (ISSM) to ensure audit findings are strictly enforced.

c. Information System Security Manager. The ISSM is the principal advisor for risk management and system authorization. The ISSM must implement and enforce the security controls required to maintain USNA's Authority to Operate (ATO) and serves as the final technical approval authority for network access. The ISSM must oversee vulnerability management and configuration control programs to mitigate enterprise-wide risk and ensure that all access aligns with the annual position audits.

d. Information Technology Services Division (ITSD). ITSD is the operational lead responsible for service delivery and infrastructure management. ITSD must provision and manage IT services and network infrastructure in accordance with defined mission priorities. ITSD must maintain the authoritative data sources for identity and access management to ensure enterprise-wide accountability and provide technical support services to ensure mission continuity for all authorized users.

e. Administrative Authorities. Leadership within the authorities, including human resources and military personnel, serves as the authoritative source for personnel status and position requirements. They are responsible for maintaining accurate, timely records within the enterprise User Repository (UR) to ensure IT access is granted or revoked based on current employment or military assignment. Administrative authorities must proactively provide the CSM with validated data to align network entitlements with official duty descriptions and background investigation statuses.

f. Authorized Users. All personnel authorized to use USNA IT resources must comply with the acceptable user policy, user agreements and all supplemental guidance issued by the CIO. All personnel are personally accountable for the protection of non-public data, including Controlled Unclassified Information (CUI) and Personally Identifiable Information (PII). Users must maintain the proactive cybersecurity vigilance required to protect the integrity and availability of the AEEE.

6. Records Management.

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located in the Department of the Navy (DON) Assistant for Administration, Directives and Records Management Division portal (https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-InformationManagement/Approved%20Record%20Schedules/Forms/AllItems.aspx).

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact your local records custodian or the USNA Records Manager.

7. Review and Effective Date. ITSD must review this instruction annually on the anniversary of the effective date to ensure continued applicability, currency, and consistency with federal, DoW, and DON policies and statutory authority, using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire ten (10) years after the effective date unless it is reissued, canceled or an extension is approved prior to the 10-year anniversary date.

8. Forms. This instruction references the following forms:

a. DD Form 2875 System Authorization Access Request

b. USNA 5230/1 Interim Access Agreement

c. USNA 5230/2 Interim Access Agreement – MIDN

d. USNA 5230/3 Privileged Access Agreement

e. Remote Use Agreement

M. J. BORGSCHULTE

Releasability and distribution: This change transmittal is cleared for public release and is available electronically only via USNA Issuances Website, https://www.usna.edu/AdminSupport/Inst/index.php.

INFORMATION TECHNOLOGY AND CYBERSECURITY POLICY AND STANDARDS

1. Definitions.

a. IT Resources. IT resources encompass any equipment, interconnected system, or subsystem used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The scope of these resources includes the following:

(1) Hardware. This includes all computing and peripheral devices, including servers, workstations, tablets, printers, copiers, smartphones, and storage devices. This also extends to infrastructure components such as routers, switches, intrusion prevention and detection systems, and traffic-shaping appliances. Support equipment, including monitors, external storage, keyboards, mice, and uninterruptible power supplies, as well as legacy communications systems like facsimile machines and pagers, are governed by this definition.

(2) Software and Firmware. This includes all operating systems, hypervisors, and applications, regardless of origin. This includes licensed commercial software, shareware, freeware, custom-developed applications, and public-domain software.

(3) Services. All functionality accessed via USNA infrastructure is included, as well as Cloud Service Provider (CSP) offerings such as Software as a Service (SaaS) and Platform as a Service (PaaS).

b. Connected Devices. Any non-traditional IT devices with network capability, including but not limited to smart facility systems, audiovisual equipment, and specialized training aids, are considered Internet of Things (IoT) or Operational Technology (OT) assets. To mitigate systemic risk, these devices must not be connected to the AEEE without first undergoing a formal security review and receiving explicit approval from the CIO. All approved IoT/OT devices must be isolated on dedicated network segments and managed in strict accordance with public law 116-207 – Iot Cybersecurity Improvement Act of 2020.

c. USNA Networks. The collective voice, video, and data infrastructure under the cognizance of the Superintendent is categorized to ensure mission-specific security, regulatory compliance, and operational efficiency.

(1) Educational Mission Network. This environment comprises IT resources on the usna.edu domain, primarily connected via the Maryland Research and Education Network (MDREN). The network is architecturally partitioned into an internal intranet for institutional operations and an extranet Demilitarized Zone (DMZ) for authorized, publicly accessible services.

(2) Military Mission Network. This environment comprises IT resources on the usna.navy.mil domain connected via the Defense Research andEngineering Network (DREN). This network supports specialized research and Department of War (DoW) interoperable requirements, adhering to stringent federal security baselines.

(3) Non-Mission Wireless Network. This is a segregated infrastructure providing controlled, direct access to the public internet for faculty and staff. This environment is intentionally distinct from the edu/mil environments to ensure that non-official activities remain isolated and do not compromise the primary mission networks. Faculty and staff are granted specific entitlements within this space to support guest sponsorship and personal productivity tools as defined elsewhere in this instruction.

(4) Non-Mission Wireless Network (RESNET). This is a segregated infrastructure providing controlled, direct access to the public internet for midshipman (MIDN). This dedicated segment ensures that MIDN personal computing and quality-of-life internet usage remain distinct from the primary mission networks to prevent impact on institutional bandwidth, security and integrity.

(5) Standalone and External Networks.

(a) Standalone Networks. Isolated environments with no external or USNA intranet connectivity. These are primarily utilized for pedagogical or research activities requiring a closed-loop system to prevent interference with the enterprise.

(b) External Networks. Commercial or governmental infrastructures utilized to support non-standard requirements through specialized, command-approved internet gateways.

d. Remote Access. Remote access is the capability of an authorized user to access USNA IT resources from an external, non-USNA controlled network (e.g., a home Internet service provider or public gateway) in accordance with reference (l).

(1) Device Compliance and Connectivity Standards. Any device utilized for remote access and connection to USNA resources must meet the minimum-security requirements, technical baselines and hardware configuration standards.

(2) Web-Based Cloud Services. Accessing authorized USNA-contracted cloud services via a standard web browser on a mobile device is generally not categorized as remote access. However, such interactions remain subject to the data safeguarding and mobile device enrollment policies specified elsewhere in this instruction.

e. Cybersecurity Workforce. Personnel assigned to the management, oversight, or operation of USNA IT resources, as defined and qualified in the reference (f).

f. Student. For the purposes of this instruction, any MIDN, Naval Academy Preparatory School (NAPS) MIDN Candidate, or domestic/foreign service academy exchange student.

g. Group Account (Positional Account). A single set of authorization credentials shared by multiple authorized users to fulfill a specific functional role.

2. Authorized Access and Users. All access to the USNA enterprise must be supported by a documented mission requirement and formal approval by the appropriate approval authorities as specified in paragraph 4. Access is granted based on the principle of least privilege, is restricted to the minimum resources necessary to perform official duties, and does not constitute an automatic entitlement to the full suite of USNA managed services.

h. User Base. The following personnel are authorized for access to the USNA information enterprise, provided they maintain the background investigation requirements and workforce qualifications required by reference (f).

(1) Standard Access. MIDN and personnel assigned to billets listed in the official USNA and NAPS Activity Manpower Document (AMD).

(2) Conditional Access. Select former civilian faculty (Emeriti), prospective AMD gains (pre-onboarding), military personnel on Temporary Additional Duty (TAD), and exchange students.

(3) Affiliated and External Personnel. Personnel from external organizations with a permanent or recurring presence at USNA, including but not limited to U.S. Navy Bureau of Medicine and Surgery (BUMED), Naval Support Activity Annapolis (NSAA), and inter-agency fellows or guest researchers, may be granted access to specified IT resources. Access for these individuals is contingent on a validated memorandum of agreement (MOA) or mission-specific justification that outlines the requirement for interoperability with USNA systems.

i. User Repository. The UR database serves as the authoritative data source for the AEEE directory, network account provisioning, and IT service entitlement.

(1) Data Integrity. To ensure compliance with reference (h), UR information must be entered and maintained by the designated administrative data owners. Responsibility for the accuracy and entry of this data rests with the Department Heads/Directors of the respective departments.

(2) Account Lifecycle. Automated provisioning and de-provisioning of accounts must be driven by UR status changes (e.g., graduation, detachment, contract termination).

(a) Reporting Timeline. Any individual departing USNA or changing status must be "end-dated" within the UR no later than 24 hours after such an official change occurs.

(b) Enforcement. This administrative entry serves as the authoritative trigger for the automated revocation of network access and the immediate reclaiming of associated IT entitlements.

(c) Accountability. Department Heads are responsible for establishing internal workflows, in coordination with ITSD, to ensure that out-processing personnel are processed immediately. Delays may create "ghost account" vulnerabilities, and failure to meet this reporting requirement constitutes a security deficiency.

2. Identity and Managed Services.

a. Identity Standards. As a DoW component, USNA must adhere to the identity management and standards established in reference (c).

(1) Persona Identifiers. To ensure clear identification of network users, display names must distinctly identify user affiliation (e.g., "mil," "civ," "ctr," "fn").

(2) Academic Exception. In accordance with the USNA's mission as a center of higher education, civilian faculty may request a waiver for standard markers. Requests for nonstandard display names must be approved by the designated authority specified herein.

b. Managed Services. Representation in the enterprise IT services directory is mandatory for all authorized users. Access to specified managed IT services is based on mission necessity and, in some cases, budgetary availability. These services include the following:

(1) Network Access. Provisioning of a mission network account on the usna.edu or Usna.navy.mil domains, establishing the primary digital identity for users within the enterprise.

(2) Cloud-based Email. Access to cloud-based email is a mission-contingent resource and is not an automatic entitlement for all personnel. Certain categories of personnel, such as Non-Appropriated Fund (NAF) employees, Naval Academy Athletic Association (NAAA) personnel, or temporary duty (TAD) military members, require a specific mission justification to receive an account. This requirement must be demonstrated and formally documented on a DD Form 2875 System Authorization Access Request (SAAR) and approved by the appropriate supervisory authority.

(3) Enterprise Information Systems. Provisioning of access to core enterprise databases and management systems (e.g., AIS, MIDS, NSTAR) based on validated "need-to-know" and specific job function requirements.

(4) Web and Content Management. Administrative and contributor accounts for USNA public-facing web resources and internal intranet servers.

(5) Storage and Collaboration. Access to enterprise-shared file systems and authorized cloud-based collaborative environments (e.g., Google Workspace, LMS) to support the academic and administrative mission.

3. Access Control and Approval Authority. Provisioning of a mission account is a mission-contingent privilege and not an automatic entitlement. Access requires formal documentation, validated mission necessity and approval by the appropriate designation authority.

a. Documentation. No access must be granted without a completed and signed authorization instrument. Depending on the user category, this includes a USNA 5230/1 Interim Access Agreement (IAA), USNA 5230/2 IAA MIDN or DD Form 2875 System Authorization Access Request (SAAR).

b. Sponsorship and Routing. Every access request must be certified by a supervisor or designated sponsor as mission-essential. To ensure institutional integrity, specific routing requirements apply to the following:

(1) Retired Faculty (Emeriti). Requests must originate from the Academic Dean and Provost and require final approval by the CIO or AO.

(2) Exchange Students. Requests must originate from the Office of the Commandant of Midshipmen.

(3) TAD Personnel. Requests must originate from the Officer Personnel Office.

(4) Students (MIDN). Requests must originate from the respective Company Officer.

(5) Group and Shared Accounts. The use of group or generic accounts is strictly controlled and authorized only by exception. Such accounts will only be considered when no individual technical solution (e.g., shared mailboxes, calendar delegation, or security groups) is feasible. All group accounts must have a designated "Sponsor of Record" who is personally accountable for the security and usage of the credential.

c. Privileged Access. In accordance with reference (f) all users granted elevated rights (e.g., administrative, root or "super-user" permissions) must be members of the Department of Defense (DoD) Cybersecurity Workforce (CWF).

(1) Training and Certification. Privileged users must be trained and certified to the appropriate level for their specific functional role. Documentation of these qualifications must be maintained in the official workforce management system of record prior to the provisioning of any elevated credentials.

(2) Requirements and Documentation. Provisioning of privileged access requires the annual submission of a USNA 5230/3 Privileged Access Agreement (PAA). This must be accompanied by a Privileged User USNA 5230/1 or a Privileged User DD Form 2875, clearly outlining the specific systems and administrative scopes required for the mission.

(3) Separation of Duties. Privileged accounts must be utilized exclusively for authorized administrative functions and must never be used for routine tasks, including but not limited to checking email, general web browsing, or the preparation of non-technical documents. Administrative actions must be performed using a dedicated privileged credential distinct from the user's standard mission account.

(4) Non-Enterprise and Research Systems. Faculty managing independent research servers or specialized laboratory environments may be granted limited privileged functions. Such access is contingent on a documented mission need, a formal risk assessment and explicit approval by the ISSM. These systems remain subject to the overarching security standards of the USNA enterprise.

(5) Revocation and Compliance. Privileged access is a continuously validated temporary grant and must be immediately revoked upon any of the following triggers:

(a) Change in CWF Status. Loss of required foundational or residential qualifier or failure to complete annual training.

(b) Mission Realignment. Transfer to a billet or role that no longer requires administrative oversight of the specified system.

(c) Security Violation. Any confirmed misuse of a privileged account, including "credential hopping" or using administrative rights for unauthorized personal or academic tasks.

(d) Administrative Separation. Notification of pending detachment or termination of employment.

d. Specialized Network Access.

(1) usna.navy.mil. Accessed via a Defense Research and Engineering Network Virtual Private Network (DREN VPN) connection initiated from a standard usna.edu user account.

(2) Remote Access. Remote access to the USNA mission and non-mission networks may be granted for administrative or end-user purposes in direct support of the USNA mission.

(a) Requirements. All users must adhere to the cybersecurity standards established in the reference (l), ensuring the remote environment and hardware meet security benchmarks for connecting to the USNA enterprise. All forms of remote access, whether client based (VPN) or web-based, require a signed Remote Use Agreement (RUA) on file prior to access authorization and use.

(b) Remote Administrative Access. This is a privileged function restricted to qualified CWF. It is reserved for resolving emergent, critical issues requiring timely response and must not be used for routine administration. Supervisors must be notified of all remote administrative sessions to ensure accountability and auditability.

(c) Remote End-User Access. Authorized for users to perform official duties consistent with their USNA position description or student status from a remote location.

e. Approval Authority. Specific authorities for granting, modifying or revoking access to USNA IT resources are designated as follows:

(1) Network Access. The Information Systems Security Manager (ISSM), or a formally designated representative, is the sole approval authority for granting access to all USNA networks (Mission, Non-Mission and Standalone). This authority ensures that all access aligns with RMF and cybersecurity requirements in accordance with reference (l)

(2) Managed IT Services. The Deputy Director of the cognizant ITSD department is the approval authority for the provisioning of managed IT services. This includes, but is not limited to, account creation for enterprise applications, email entitlements, and cloud service allocations.

(3) Executive Approval. The CIO, or a formally designated representative, is the final approval authority for all IT service requests submitted by retired USNA faculty. This oversight ensures that the limited resources provided to retired personnel remain in direct support of USNA's academic mission outlined in the reference (i).

(4) Revocation Authority. All approved authorities reserve the right to summarily suspend or revoke access if a user is found in violation of any user agreement or if a security vulnerability is identified, in accordance with reference (c).

4. Authorized Use.

a. Definition. Authorized use is the utilization of IT resources in direct support of the USNA mission in a manner that complies with all applicable laws, regulations, and command policies.

(1) Determination. Users must not unilaterally determine what constitutes "authorized use." Any ambiguity regarding the appropriateness of a specific activity must be resolved by the appropriate supervisor in consultation with the ISSM.

(2) Professional Conduct and Social Media. Access to social media and other public-facing digital platforms via USNA IT resources is permitted only as authorized for mission-related purposes or limited personal use. All digital interactions must adhere to the professional standards of the DON and must not compromise the operational security or integrity of the USNA networks. Official representation of USNA on any digital platform is restricted to designated personnel and must align with the established public affairs guidance.

(3) Consent to Monitoring. In accordance with reference (d), by accessing any USNA IT resource, users acknowledge and consent to the terms specified in the standard DoW login banner. This consent extends to all IT services, including cloud-based applications accessed via mobile devices or remote connections, regardless of geographic location or ownership status of the endpoint device.

b. Limited Personal Use. In accordance with reference (c) and at the discretion of the respective cost center head, personnel may be granted limited personal use of IT resources. Such use is a privileged, not a right, and must adhere to the following criteria:

(1) Will not adversely affect the employee's performance of official duties or network bandwidth.

(2) Will be of reasonable frequency and duration, occurring primarily during personal time (e.g., lunch breaks).

(3) Will serve a legitimate interest that indirectly supports the USNA mission, such as enhancing morale or professional development.

(4) Will not incur additional costs to USNA or the U.S. Government.

(5) Will be continuously attended and compliant with all cybersecurity protocols.

c. Portable Computing Devices. Government-Furnished Equipment (GFE) provided for institutional use may be utilized outside the traditional workplace (e.g., during official travel or authorized remote work) under the following conditions:

(1) Supervisory Approval. Off-site utilization of GFE must be explicitly authorized by the employee's supervisor. In the absence of a formal telework agreement, the removal of GFE from the USNA perimeter is considered temporary and for specific mission requirements; GFE is provided for official duties and must not be utilized as a permanent personal or home computing resource.

(2) International Travel and Security. To mitigate foreign intelligence and technical threats, the Deputy Director for Cybersecurity, ITSD, must be notified by the respective administrative authority in advance of any international travel involving a GFE. All devices transported internationally are subject to mandatory security inspection and re-imaging by ITSD upon return to USNA before reconnection to the mission network must be permitted.

(3) Standards of Care. Personnel are personally accountable for the physical security and date integrity of GFE in their possession. Devices must be managed in accordance with the hardware standards and protective measures defined in the reference (l).

5. General User Responsibilities. The prudent, efficient, cost-effective, and secure use of IT is a professional obligation. All users must comply with the acceptable use policy for USNA IT resources and the navy user agreement and consent provisions. Beyond those baseline requirements, users must adhere to the following standards:

a. Users are expected to maintain a level of digital literacy sufficient to perform basic computing tasks without routine technical assistance.

b. Users must proactively obtain the training necessary to operate systems required to perform their assigned duties. This includes completion of the annual DoW IA Training (Cyber Awareness Challenge), review of system-specific manuals or command-approved tutorials and adherence to the qualification standards set forth in the DON Cyberspace Workforce Program (reference (c)) for those in designated CWF roles.

c. Enterprise storage and network bandwidth are limited government resources. Users must minimize data duplication and follow the records retention schedules outlined in the DON Records Management Program (reference (h)). Users must understand which directories are covered by enterprise backup services. Users are responsible for the backup of critical mission data stored outside of these managed environments (e.g., local research data).

d. All personnel must execute the following best practices to defend the security and integrity of the USNA networks:

(1) Mandatory Incident Reporting. Immediately reporting any suspected cybersecurity incident or anomalous activity to the ITSD Web Help Desk via phone or email. This includes, but is not limited to, suspected phishing, unusual system behavior, malware indicators, or the loss of theft of any device containing USNA data. Delays in reporting significantly increase the risk to the enterprise and may result in administrative revocation of access.

(2) Electronic Communication Safety. Exercise extreme caution with attachments or messages from unknown or unexpected senders. Users must not interact with shortened or unverified links contained within emails or on websites without first confirming the legitimate link destination.

(3) Software and Content Integrity. Strictly adhere to the established procurement and installation policies. Refrain from downloading, installing or executing software, firmware or digital content from untrusted, non-DoW approved or unauthorized external sources. All software utilized on the AEEE must be verified against the functional baseline and comply with the security standards defined in reference (m) and the CCB process.

(4) Credential Management. Adhere to strict identity protection standards by never reusing passwords or passphrases across multiple accounts. This reuse of credentials between personal systems and government IT systems is strictly prohibited

(5) Data and Device Safeguarding. Ensure that all institutional data remains on authorized hardware within approved secure environments. Personnel are responsible for the physical security of any government furnished equipment in their possession and must ensure that non-public data is never processed on unmanaged or personal devices.

6. IT Life Cycle Management (LCM).

a. LCM Worksheets and Abbreviated System Decision Paper (ASDP). Per reference (i) the annual updating of LCM worksheets and accompanying ASDPs are the primary vehicle for planning all IT requirements. All IT resource requirements must be documented annually within each Cost Center's LCM worksheet and an ASDP, which must explicitly identify any dependencies on reimbursable or gift-funded resources. Any requirements arising outside the annual cycle must be documented as a formal amendment to the existing LCM worksheet to ensure continuous alignment with enterprise architecture.

b. Supply Chain Risk Management (SCRM). All IT acquisitions, regardless of funding source, must undergo a SCRM assessment in accordance with reference (a). This process verifies the provenance and integrity of hardware, software, and firmware to mitigate risks from foreign intelligence services, counterfeit components, and other supply chain threats. No IT resource can be introduced into the environment without a validated assessment of its supply chain integrity.

c. Acquisition and Procurement. All IT acquisitions must receive LCM approval by the Deputy Director for ITSD prior to purchase. Requesting organizations are responsible for providing complete and accurate specifications, impact assessments, and configuration control board artifacts to ensure every procurement action is technically sound, fiscally authorized, and compliant with the security standards established in this instruction.

d. Funding Streams.

(1) Capital and New Assets. New or improved IT capabilities must be funded through Other Procurement, Navy (OPN) or Operations and Maintenance (O&MN), as appropriate for the asset class.

(2) Sustainment. Routine maintenance and operational support for existing IT assets must be funded through the centralized O&MN maintenance account.

(3) Consumables. Consumable supplies, non-centralized maintenance, and incidental software acquisitions are the responsibility of the requesting organization and must be funded from organizational O&MN expense accounts.

(4) Gift and Reimbursable Funding. Acquisitions funded through gifts or reimbursements must include a commensurate sustainment plan. This plan must cover the full life cycle costs of non-standard or enhanced technologies to ensure that gifted capabilities do not create unfunded requirements for USNA in future fiscal years.

(5) Asset Accountability. In accordance with the reference (k), property responsible officers must be designated within each department to maintain an accurate and continuous inventory of all departmental IT assets. All assets must be tracked from initial receipt through final disposition or survey. Any lost, damaged or stolen IT assets must be reported immediately to the proper authorities in accordance with established property management regulations.

7. World Wide Web.

a. Web Administration and Oversight. The official USNA internal (Intranet) and external (www.usna.edu) websites are administered by ITSD, who provides the underlying architecture, hosting environments and technical assistance for all institutional web properties to ensure high availability and security.

b. Content Clearance and Privacy. The Public Affairs Office (PAO) serves as the primary authority for the strategic direction and final approval for all public-facing content. All information intended for the external USNA website must be cleared for public release by the PAO in accordance with reference (b). This review process is mandatory to ensure no sensitive, non-public, or CUI is exposed to the public domain.

c. Distributed Maintenance. Specific website subsections or departmental pages may be maintained by designated content developers outside of ITSD. These individuals must be responsible for the accuracy and currency of the information within their designated areas. All content developers must comply with ITSD technical standards before being granted write-access to web directories.

d. Records Management and Compliance. Web content documenting official USNA business, policy, or institutional history is a federal record and must be managed in accordance with reference (h). All web properties must adhere to the supplemental guidance and detailed standards published on the intranet, including Section 508 accessibility requirements, as well as the hardware and software standards defined in reference (l).

8. Exchange Students.

a. Service Provision. ITSD is responsible for providing IT services for all visiting students, including domestic students participating in the service academy exchange program and to foreign national students identified and authorized by the Academic Dean and Provost.

b. Organizational Responsibilities. To ensure exchange students are fully operational prior to the start of the academic semester, the following coordination is required:

(1) Military Oversight. The Commandant of Midshipmen must manage the military affairs of all students, serving as the primary validator for network access requests.

(2) Hardware Logistics. USNA Business Service Division (NABSD) must issue, track and maintain student computing devices.

(3) Network Integration. ITSD must ensure all students are represented in the UR and enterprise directory to enable access to learning tools and management systems.

c. Procedural Alignment. Coordination between the Academic Dean and Provost, the Commandant, NABSD and ITSD must be conducted in accordance with the timelines and procedures established in enclosure (2). This includes the mandatory "foreign national" vetting process for foreign national students per references (a) and (i).

9. Cybersecurity and Configuration Control.

a. Authority to Operate (ATO). In accordance with the Federal Information Security Management Act (FISMA) and reference (l) all USNA IT's must undergo a formal security assessment and authorization process. The USNA ATO is specifically tailored to an educational environment as defined in reference (g). Authorization is not a one-time event; it requires continuous monitoring and periodic reassessment to ensure the risk posture of the system remains acceptable.

b. Device and Software Controls. To safeguard the USNA mission network, the following restrictions apply:

(1) Unauthorized Hardware. Connectivity of personally owned devices (e.g., laptops, servers, or network appliances) to the mission network infrastructure is strictly prohibited without prior written authorization from the ISSM.

(2) Mobile Device Registration. Personally owned mobile devices used to access USNA-contracted cloud services or institutional data must be enrolled with the designated device management authority. Users must adhere to all enrollment requirements, including mandatory authentication standards and the enforcement of security policies. The loss or theft of any enrolled mobile device must be immediately reported to the ITSD Help Desk.

(3) Threat Mitigation and Quarantine. ITSD maintains the authority to proactively manage devices connected to the AEEE to mitigate cybersecurity threats in accordance with reference (m).

(a) GFE. GFE found in violation of security baselines or actively compromised are subject to immediate quarantine, reconfiguration or physical seizure by ITSD.

(b) Personally Owned Devices. Personally owned devices identified as a threat will be immediately quarantined via network-level isolation. Access to institutional resources will remain revoked until the device is confirmed to be remediated and compliant with minimum connectivity standards.

(c) Software Compliance. Vulnerable software or applications without an approved mitigation plan or remediation timeline must be disabled or removed from the environment to ensure continuous mission assurance.

c. Configuration Management.

(1) Baseline Integrity. All system configurations must be maintained in a standardized and secure configuration in accordance with reference (g). No modifications to established system baselines, hardware architectures, or software environments are permitted without formal authorization. Unauthorized or "ad hoc" changes to any component on the mission network are strictly prohibited and may result in the immediate disconnection of the affected resource.

(2) Configuration Control Board (CCB). The CCB serves as the primary governance body for the technical evolution of the enterprise. Any significant modification to the network architecture, security posture, or functional baseline must be formally submitted, reviewed, and approved through the CCB process prior to implementation.

(3) Implementation Procedures. Technical procedures for configuration management, including the specific criteria for "significant change" and the lifecycle of change requests, are promulgated and managed by ITSD. All personnel, including system administrators, developers, and personnel managing research environments, must adhere to these procedures to ensure continuous interoperability and security across USNA.

d. Workforce Readiness. In accordance with reference (f), members of the CWF must maintain all required qualifications, failure of which must result in immediate revocation of privileged access or administrative action.

10. ITSD Support and Service Tiers.

a. Support Priorities. ITSD must manage the acquisition, operation, and maintenance of IT assets based on mission impact. Resource must be allocated according to the following priority order:

(1) Emergent Critical. System-wide failures, disaster recovery and immediate threat mitigation.

(2) Externally Driven. Mandates from higher authority, including legal, regulatory or cybersecurity requirements.

(3) Enterprise Mission Systems. Core infrastructure and contracted services including MIDS, AIS, NSTAR, cloud services.

(4) Academic Core. Systems supporting the core curriculum courses.

(5) Academic Major and Research. Major-specific electives and faculty research initiatives.

(6) Administrative and Command Support. Research, conferences, and extracurricular activities.

b. Service Centers. The Information Technology Service Center (ITSC) and Academic Technology Service Center (ATSC) serve as the primary points of contact for all IT requests.

(1) Scope and Submission. Support is limited to managed IT services and resources. The ITSC does not provide basic computer literacy training, support for non-standard third-party software or physical maintenance for student computing devices. Requests may be made via telephone, email (for help desk ticket entry), or in-person at the ITSC or the ATSC.

(2) Support Levels and Escalation:

Tier	Description	Target Resolution
Level 1	Routine issues resolved via telephone, remote assistance, or walk-in.	Same business day (during normal hours).
Level 2	Complex issues requiring single-department expertise or data analysis.	1-3 business days.
Level 3	Issues requiring new solutions or cross-departmental coordination.	7 business days.

c. Procurement-Dependent Issues. Requests to support issues requiring acquisition to or configuration changes of a new IT solution for resolution must transition to the LCM process in accordance with reference (f) and may require review by the CCB to ensure compliance with reference (b).

11. Accessing and Safeguarding USNA Data. Users are individually accountable for the protection of the confidentiality, integrity and availability of USNA data. In accordance reference (h), data is categorized by sensitivity level and must be managed accordingly to prevent unauthorized disclosure or compromise. Information specifically approved for public release in accordance with the DoD Information for public release per reference (l).

a. Non-Public Data. Non-public data, including CUI and PII) must reside exclusively on authorized USNA IT resources. PII of USNA personnel as well as other USNA-associated CUI must never be stored on a personally owned device under any circumstance. When accessing non-public data from an external network (e.g., home ISP), the following apply:

b. Web-Authenticated Access. Access to non-public data via a web browser on a personally-owned device is strictly prohibited. Such data may only be accessed from a non-GFE device through a command-approved secure environment, such as a USNA-hosted virtual desktop (VDI) or other solution that isolates data from the local machine.

c. Secure Connection Requirements. In all other instances, users must employ one of the following secure methods:

(1) Use of the USNA VPN is required.

(2) Access must be conducted via a Remote Desktop (RDP) connection, a USNA hosted VDI, or a secure command-line interface.

d. Device Hierarchy and Hardware Standards. Users must utilize GFE for all official business whenever available. Specific technical standards for GFE, including the authorized use of removable media, peripheral connectivity, and the management of telework IT suites, are established in reference (b).

(1) Users with an approved telework agreement must utilize the designated telework IT suite as their primary interface with USNA IT resources.

(2) If GFE is unavailable, a personally owned device may be utilized only for the preparation of non-sensitive academic materials (e.g., lesson plans, research papers).

(3) Personally owned devices must never be used for the processing, manipulation, or storage of CUI, PII, or sensitive administrative records. All hardware interactions remain subject to the security configurations and acceptable use standards.

e. Artificial Intelligence (AI). Personnel are prohibited from inputting non-public data or internal communications into any public or non-USNA-approved AI service, platform or application. Use of any AI tool for official duties must be explicitly authorized by the CIO. Authorized AI implementations must be risk assessed and ensure that data remains within the secure USNA perimeter and is not utilized for training external or public models.

PROVIDING IT ASSETS, SERVICES, AND SUPPORT TO EXCHANGE STUDENTS

1. Academic Dean and Provost. Before the start of each academic semester, the Academic Dean and Provost must:

a. Provide ITSD and NABSD the number of computing devices required by foreign exchange students.

b. Ensure each foreign exchange student has an established record in the USNA enterprise MIDS system.

2. The Commandant of Midshipmen. Before the start of each academic semester, the Commandant of Midshipmen must:

a. Provide NABSD with the number of computing devices required for domestic exchange students for asset and systems support planning purposes.

b. Ensure each inbound domestic exchange student has an established record in the USNA enterprise MIDS system to permit assignment of IT services.

c. Initiate a DD Form 2875, System Authorization Access Request (SAAR), for all exchange students, foreign and domestic.

d. Provide ITSD with any special computer configuration requirements specified by the exchange student's source organization for consideration in network configuration control (e.g., VPN client software and configuration required for online coursework or course registration).

e. Ensure that all issued IT assets are returned to NABSD to support efficient life-cycle management prior to an exchange student's return to the source organization.

3. Naval Academy Business Services Division (NABSD). The Director, NABSD, must:

a. Coordinate with ITSD to provide IT assets with hardware and software functionally equivalent to those issued to an exchange student's USNA year group.

b. Ensure sufficient computing devices are available prior to each academic semester to support the number of exchange students identified by the Academic Dean and Provost and the Commandant of Midshipman.

c. Provide exchange students with the same computer support services provided to all USNA midshipmen.

4. Information Technology Services Division (ITSD). The Deputy, ITSD, must:

a. Coordinate the transfer of computer custody between NABSD, ITSD and exchange students.

b. Grant exchange students standard network services equivalent to those provided to all USNA midshipmen.

c. When practicable, accommodate special computing configurations required by the exchange student's source organization, subject to configuration control and cybersecurity requirements.