Department of the Army
Headquarters, U.S. Army Cadet Command
1st Cavalry Regiment Road
Fort Knox, Kentucky 40121-5123

USACC Regulation 25-1

Effective 01 May 2018

Information Management

U.S. ARMY CADET COMMAND INFORMATION AND INFORMATION TECHNOLOGY EQUIPMENT HANDLING

FOR THE COMMANDER:

OFFICIAL:

CHRISTOPHER P. HUGHES
Major General, U.S. Army
Commanding

JANET R. HOLLIDAY
Colonel, GS
Chief of Staff

History. This publication is a new U.S. Army Cadet Command (USACC) regulation.

Summary. This regulation makes permanent USACC policy for the handling of information and Information Technology (IT). All IT policy letters listed in Appendix B are rescinded by this regulation.

Applicability. This regulation applies to Headquarters, USACC and its subordinate units.

Proponent and Exception Authority. The proponent for this regulation is the USACC Deputy Chief of Staff, G6 (DCS, G6). The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling laws, regulations, and USACC policies. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent.

Army Management Control Process. This regulation does not contain management control provisions.

Supplementation. Supplementation of this regulation and establishment of local forms are prohibited by subordinate commands of USACC.

Suggested Improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQ, USACC, ATTN: ATCC-IT, Fort Knox, KY 40121-5123.

Distribution. Distribution of this regulation is intended for HQ USACC and its subordinate units. Distribution is in electronic format only.

Summary

USACC Regulation 25-1
U.S. Army Cadet Command Information and Information Technology Equipment Handling

- This regulation makes permanent USACC policy for the handling of information and IT with all IT policy letters listed in Appendix B rescinded. This regulation does not add USACC level regulatory guidance to all areas covered within the rescinded policy letters. In those cases command personnel must refer to published higher guidance.

Contents

Chapter 1 – Introduction 1
1-1. Purpose 1
1-2. References 1
1-3. Explanation of Terms 1
1-4. Responsibilities 1
Chapter 2 – IT Governance 4
2-1. General 4
2-2. Structure and Process 4
Chapter 3 – Cyber Security 5
3-1. Sensitive and Classified Information Spillage 5
3-2. Data Security 5
3-3. Incident Handling and Response 6
Chapter 4 – Information Systems and Mobile Devices 7
4.1 Information Technology Equipment Authorization 7
4.2 Labeling USACC Mobile-Portable Electronic Devices 7
4.3 Responsibility for Government Issued Wireless Internet Devices 8
4.4 Computer Hard Disk Drives (HDD) and Media Destruction, Storage, and Reuse 8
Chapter 5 – Command-wide Standard for Electronic Mail 10
Chapter 6 – Command Responsibilities for Freedom of Information Act (FOIA) Requests 13
6.1 The Freedom of Information Act (FOIA) 13
6.2 The Privacy Act of 1974, as amended, 5 U.S.C. § 552a 13
6.3 The Request Process 13
6.4 Case Management 14
6.5 Format 15
6.6 Supporting Documents 15
6.7 Training 15
Chapter 7 – Official Mail 17
APPENDIX A – References 18
Section I – Referenced Publications 18
Section II – Prescribed Publications 19
APPENDIX B – Rescinded IT Policy Letters 20
GLOSSARY 21
Section I – Acronyms and Abbreviations 21
Section II – Terms 23

Chapter 1 – Introduction

1-1. Purpose

This regulation establishes USACC policies and assigns responsibilities for the governance of information and information technology handling. It implements the Command, Control, Communications, Computers, and Information Management (C4IM) provisions outlined in AR 25-1, AR 25-2, other Army regulations and Department of Defense Directives.

1-2. References

References are listed in Appendix A.

1-3. Explanation of Terms

Acronyms and special terms used in this regulation are in explained in the Glossary.

1-4. Responsibilities

a. USACC, Commanding General (CG).

(1) Overall responsibility for conducts of Information Management/Information Technology IM/IT program; delegating the authority for management to the DCS, G6.

(2) Decision authority for, or appoints a representative to, the USACC IT Change Control Board (CCB).

b. Brigade Commanders.

(1) Assign responsibilities to execute and support brigade (BDE) IM/IT processes and programs.

(2) Comply with acquisitions processes and reporting requirements as stated throughout this regulation. Submit documentation to USACC Chief Information Officer (CIO) for acquisitions outside local approval authority.

(3) Coordinate requests for projects that include IM/IT with USACC CIO for technical review and approval.

(4) Assign responsibility for records management per AR 25-400-2.

(5) Assign responsibility for primary and alternate Official Mail Manager(s) who will be responsible for reporting all postal expenditures that are paid for by government funds.

(6) Assign a primary and alternate SharePoint Champion(s) to manage BDE user permissions.

(7) Ensure that their BDE's IT asset information is current in the IT Asset Management Database.

(8) Ensure their BDE's IT requirements are current and any new requirements are submitted using the Information Technology Equipment, Products, and Services (ITEPS) process.

c. Directorate Heads.

(1) Ensure their Directorate's IT requirements are current and any new requirements are submitted using the ITEPS process.

(2) Coordinate management decision documents for all service contracts with an IM/IT component with the USACC CIO/G6.

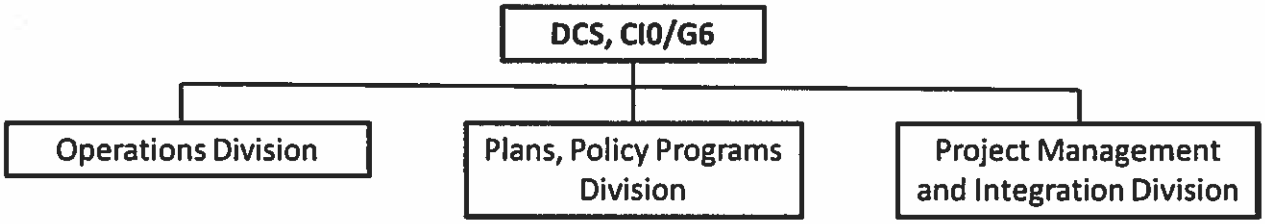
(3) Attend or assign a representative to attend, the USACC IT CCB and Change Advisory Board (CAB).

(4) Coordinate requests for projects that include IM/IT with USACC CIO for technical review and approval.

(5) Assign a primary and alternate Records Coordinator to maintain records in accordance with AR 25-400-2.

(6) Assign a primary and alternate SharePoint Champion to manage directorate user permissions.

d. Chief Information Officer/G6.


DCS, CIO/G6
Operations Division
Plans, Policy Programs Division
Project Management and Integration Division

(1) Establish policy for the management of information resources and the programming, funding, and acquisition of IM/IT equipment and services.

(2) Develop guidance and plans for managing IM/IT investment strategies. Advise the USACC Administrative Contract Review Board (ACRB) and the USACC Senior Leadership in the prioritization of IM/IT requirements for funding.

(3) Assist the Knowledge Management (KM) to deliver knowledge management capabilities for the successful planning, integration, and execution of knowledge management throughout the command.

(4) Assist the Deputy Chief of Staff, G4 (DCS, G4) in all areas of IM/IT acquisitions to achieve desired level of services across USACC.

(5) Assist the Deputy Chief of Staff, G8 (DCS, G8) in identifying Program Objective Memorandum (POM) requirements, determination of appropriate use of Operation Maintenance, Army (OMA)/Other Procurement and Army (OPA) funding for IM/IT acquisitions.

(6) Coordinate with Office of the Army CIO/G6, Network Enterprise Technology Command (NETCOM), Training and Doctrine Command (TRADOC), Human Resources Command (HRC) and the Installation Management Agency (IMA) regarding provisioning of enterprise and common user IM/IT services.

(7) Manage the process for IM/IT acquisitions that require Headquarters (HQ) USACC approval to include requirements that will incur a recurring obligation, for example, long haul communications services, desktop video teleconferencing, monthly/yearly user fees and other recurring IM/IT service accounts.

(8) Manage the Command Cyber Security (CS) Program, per Army Regulation (AR) 25-2 and TRADOC Supplement 1.

(9) Provide the Command Webmaster, Records Manager and Publications.

(10) Acts as the Co-Chair for, or appoints a representative to, the USACC IT CCB.

(11) Acts as the Review and Concurrence Authority for, or appoints a representative to, the USACC IT CAB.

(12) Act as approving authority for all requests to store government-owned data on non-government systems or media.

(13) Establish, and ensure availability of, the IT Asset Database.

Chapter 2 – IT Governance

2-1. General

IT Systems Change Management is comprised of the Change Advisory Board (CAB) and the Change Control Board (CCB), the process of which is outlined in the Information Technology (IT) Enterprise Change Management (ECM) SOP. The IT ECM SOP is located in the USACC Knowledge Center.

2-2. Structure and Process

a. A CAB will be established with the CIO/G6, or designated representative, as the Review and Concurrence Authority and the G6 Project Management Integration Division (PMID) Chief as the chairperson. The CAB will address all significant and emergency changes to USACC C4IM services portfolio. The purpose of the CAB is to discuss the proposed changes with the participants of the meeting, resolve any conflicts or issues and develop a draft priority of work effort. The output of this meeting feeds the CCB. The charter for this board will be written by the USACC G6 PMID and approved by the CAB.

b. A CCB will be established with the USACC CG, or designated representative, as the Decision Authority and the CIO/G6 as the chairperson. The CCB will address all significant and emergency changes to USACC C4IM services portfolio. The purpose of the CCB is to review the proposed changes/modifications and priority, discuss any concerns, adjust priority and approve the overall work effort. The charter for this board will be written by the USACC G6 PMID and approved by the CCB.

c. The directorate heads or their designees of the following organizations will attend both the CAB and CCB as voting members: G1; Recruiting, Marketing and Incentives Directorate (RMID); G3; G4; Directorate of Leader Development and Education (DoLD-E); G6; G8; Knowledge Management Office (KMO), and Junior ROTC.

d. Any organization that submits a Request for Change (RFC) will assign an Action Officer (AO) to work with the G6 PMID AO in developing the RFC for presentation to the CAB and CCB.

Chapter 3 – Cyber Security

3-1. Sensitive and Classified Information Spillage

a. Spillage occurs when sensitive and/or classified information is processed or received on an unclassified Information System (IS), or on a classified system operated at a lower level of classification than the information that was received. Most spillage incidents are a result of careless methods, shortcuts, or untrained users who have intentionally or accidentally compromised sensitive and/or classified information. When spillage of sensitive and/or classified information happens, immediate action is required to minimize any damage and eliminate any conditions that might cause further compromises.

b. All spillages of sensitive and classified information will be handled in accordance with the USACC Incident Response Plan located in the USACC Knowledge Center.

3-2. Data Security

a. Storage of all government data is restricted to government owned or managed devices. All government data, including e-mail, business notes, and calendar information, will not be copied to non-government owned data drives, personally owned devices that do not have government owned mobile device management software installed, or commercial web storage services such as the Apple iCloud or to non-government owned storage devices. The USACC CIO/G6 is the only authority that can grant exceptions to the restrictions outlined in this paragraph.

b. Government electronic mail (e-mail) that contain Personally Identifiable Information (PII), sensitive information, or official business are restricted to government managed e-mail systems. Government e-mails that contain PII, sensitive information, or official business will not be copied, forwarded, or transferred in any way to non-government owned systems, accounts, or data drives. E-mails that contain information on public events or personal correspondence can be copied, forwarded, or transferred to non-government systems by the email sender or recipient as long as they are examined and purged of any potential PII, sensitive information and official business first.

c. Government e-mail archives (Outlook files with a Personal Storage Table (PST) file extension) may not be copied to non-government owned data drives or web-storage services. USACC personnel (military, civilian, and contractor) are not allowed to retain their PST file extension when leaving their service or employment with the command without G6 approval.

d. USACC personnel working remotely (i.e., not at permanent place of duty) will only utilize Government Furnished Equipment (GFE) to access government networks, and access will be via Virtual Private Network (VPN) "tunnel". Log in to the GFE will be with Common Access Card (CAC) only.

3-3. Incident Handling and Response

a. Incident response, to include PII breach, is the responsibility of personnel at the headquarters, brigade, and program level. Information system and network incidents include, but are not limited to, an assessed event of attempted entry, unauthorized entry, and/or an attack on an automated information system, to include unauthorized probing, browsing, disruption, or denial of service.

b. The USACC G6 Incident Response Plan defines the responsibilities and actions of staff who may be involved in responding to incidents involving IT or IS assets and outlines the responsibilities and actions of the Human Resources Command (HRC) Cyber Security Division (CSD) and their role as the service provider. For complete information, please reference the USACC G6 Incident Response Plan, HRC's Incident Response Plan Standard Operating Procedures (SOP) for Recruiting Services Network (RSN) and USAHRC Components on the Fort Knox Installation Campus Area Network and the HRC/USACC Service Level Agreement.

Chapter 4 – Information Systems and Mobile Devices

4.1 Information Technology Equipment Authorization

a. The IT equipment type and quantities described in the USACC IT Equipment Authorization Spreadsheet are authorized for acquisition through approved channels and issue, if necessary, within the command. The USACC Equipment Authorization Spreadsheet is derived from the Basis of Issue Plan (BOIP) and the Common Table of Allowances (CTA 50-909). The number and type of IT equipment are directly linked to the organization's personnel totals, roles and operational requirements and adhere to command budget guidance. Requests for authorized IT equipment shall be submitted using the ITEPS process. Information about the ITEPS process can be found in the USACC G6 Public Documents section in SharePoint.

b. USACC organizations may request an exception to policy to meet mission-essential, operational and/or organizational requirements. All requests must be submitted using the ITEPS process. The USACC G6 retains staff oversight of the IT equipment authorization exception to policy process.

c. USACC headquarters staff sections will identify and submit their new or changed IT requirements to the USACC G6 NLT the end of the 3rd Quarter of each fiscal year (3QTRFY). USACC Brigades will identify and submit new or changed IT requirements for the brigade headquarters and all programs that fall under their purview NLT the end of 3QTRFY. The USACC G6 will conduct an IT equipment authorization/BOIP review every 4th quarter of each fiscal year to facilitate the next fiscal year's life cycle. Additionally, the USACC G6 will conduct an IT equipment authorization/BOIP review when IT requirements change significantly, with substantial IT equipment fielding, or when the TDA changes. The USACC G6 will validate command IT requirements and if necessary, update the IT Equipment Authorization Spreadsheet to reflect evolving requirements.

d. The USACC G6 will utilize the IT Asset Management Database to determine the IT equipment for lifecycle. This database provides USACC organizations an administrative tool for proper management of their IT equipment by facilitating the organization's ability to track location, purchase date, warranty information, and other information that simplifies lifecycle planning. All USACC organizations will ensure that the IT Asset Management Database is updated as changes occur. Additionally, HQ and brigades will provide any necessary training or permissions for or to the database for HQ, brigade, or subordinate staff.

4.2 Labeling USACC Mobile-Portable Electronic Devices

Guidance for approving Portable Electronic Devices (PED) for travel is as follows:

a. All government owned or leased laptops, PEDs, and removable storage media must be protected using an Army-approved Data at Rest (DAR) encryption solution or active and supported file based encryption. If the device does not have an Army-approved DAR or file based encryption solution, then it is not approved for travel.

b. All PEDs that have an Army-approved DAR encryption solution will have a label on them approving them for travel, before they leave the unit. In order to avoid advertising these devices as government systems containing sensitive information, a USACC Label 3 is affixed to the inside of the laptop computer in the lower left corner just below the keyboard and a USACC Label 2 will be affixed in an inconspicuous place on the smaller PEDs, such as smartphones, and other portable media. The labels will state that they comply with the Army data encryption standard and are authorized for travel.

c. Mobile devices issued at the Headquarters (HQ) USACC level will be labeled by the G6 IMO. BDE IMOs have authority to place the labels on devices received at the BDE level. ROTC Program Information Assurance Security Officers (IASO) have the authority to place labels on devices received at the ROTC Program level. It is, however, the responsibility of the user to ensure their device is properly labeled. If the IMO or IASO does not have labels on hand, the label templates in .pdf are located in the USACC Knowledge Center.

d. The USACC Label 2 dimensions are ½" x 1 ¾" and have 80 labels per sheet. Blank sheets can be attained through the appropriate supply channels.

e. The USACC Label 3 dimensions are 1" x 2 ⅝" and have 30 labels per sheet. Blank sheets can be attained through the appropriate supply channels.

4.3 Responsibility for Government Issued Wireless Internet Devices

a. Individuals who sign for government owned wireless internet device (i.e., MiFi) will be held responsible for loss or damage to the device regardless if it is through negligence or willful act. Additionally, wireless internet devices will not be given or issued to non-USACC associated individuals, including Cadets.

b. All individuals using government owned wireless internet devices must conduct themselves in accordance with their signed Acceptable Use Policy (AUP), DoD, and Army policies.

4.4 Computer Hard Disk Drives (HDD) and Media Destruction, Storage, and Reuse

a. Personnel performing the purging and/or degaussing process on HDD or media will be appointed on an authorization memorandum (USACC Media Sanitation and Destruction SOP). Duty appointment letters will be maintained by the IMO/S6.

b. The IMO/S6 will verify that authorized personnel are trained on the purging and/or degaussing process.

c. Approved Software Tool:

(1) The Universal Purge Tool (UPT) is a tool used to overwrite data on various types of storage media. Once overwritten by the UPT, the data becomes irrecoverable through standard means such as the use of recovery software. The UPT is an Army owned IA tool and should be controlled by an authorized IASO or IMO.

(2) The UPT and corresponding manual documentation can be obtained by contacting the USACC G6.

d. Purging, Degaussing, and Physical Destruction: The processes by which the IMO/S6 will conduct purging, degaussing, and physical destruction of USACC operated media are outlined in the USACC Media Sanitation and Destruction SOP located in the USACC Knowledge Center.

(1) Personnel performing the purging and/or degaussing process on HDD or media will be appointed on an authorization memorandum (USACC Media Sanitation and Destruction SOP). Duty appointment letters will be maintained by the IMO/S6.

(2) The IMO/S6 will verify that authorized personnel are trained on the purging and/or degaussing process.

Chapter 5 – Command-wide Standard for Electronic Mail

a. Military, civilian, contractor, and foreign national personnel assigned to or who work in support of the command will use Defense Information Systems Agency (DISA) Enterprise E-mail, or other Army G6 approved e-mail capability to communicate in their official capacity for USACC and the Army.

b. In accordance with AR 25-1, the use of commercial e-mail accounts for official purposes are prohibited (to include .edu e-mail accounts). Automatically forwarding from an official government account to an unofficial account (commercial service) is prohibited. Automatically forwarding of official e-mail to non-official or non-secure devices is prohibited.

c. Personnel will use the following standard for e-mail messages and signature block format on all e-mail correspondence:

(1) Signature Block: All military, civilian, contractor, and foreign national personnel will utilize a standard signature block to identify the writer's rank or grade and position along with required contact information. When writing any type of correspondence, the signature block's required contact information will identify the writer by name, military rank or civilian grade, command, duty position, telephone number, and if appropriate, facsimile number (optional) and e-mail address. Military personnel will use their rank as their identifier.

Example:

Ralph F. Smith, SSG
U.S. Army Cadet Command, G1
DSN: 464-0000
Telephone: (502) 624-0000
Fax: (502) 624-0000
Ralph.F.Smith11.MIL@mail.mil

(2) All Department of the Army civilian employees will be identified by pay plan (GS, YA, SES, or WG), pay grade if desired, duty position, and organization along with required contact information.

Example:

James C. Smith, GS
Deputy Director, G7
U.S. Army Cadet Command
DSN: 464-0000
Telephone: (502) 624-0000
Fax: (502) 624-0000

James.C.Smith8.CIV@mail.mil

(3) All contractor personnel will utilize a standard signature block to identify the writer as a contractor, their associated duty position/organization, and company name along with required contact information.

Example:

John E. Maramack, Contractor
Strategic Planner, G5
U.S. Army Cadet Command
Contracting Company Name
DSN: 464-5555
Telephone: 502-624-5555
John.E.Maramack3.CTR@mail.mil

(4) All foreign national personnel will utilize a standard signature block to identify the writer's name/rank, duty position/organization, and country of origin along with required contact information.

Example:

George S. Martinez
Strategic Planner, G5
U.S. Army Cadet Command
Canada
DSN: 464-5555
Telephone: 502-624-5555
George.S.Martinez.FN@mail.mil

(5) All foreign national contractor personnel will utilize a standard signature block to identify the writer's name, affiliation as a contractor, duty position/organization, country of origin, and company name along with required contact information.

Example:

Gregory S. Abboud, Contractor
Strategic Planner, G5
U.S. Army Cadet Command
India
Contracting Company Name
DSN: 464-5555
Telephone: 502-624-5555
Gregory.S.Abboud.FN@mail.mil

d. Any additional name or designation on signature blocks is prohibited. The use of any type of motivational message is prohibited. Icons and logos add unnecessary overhead to the message and are not authorized.

e. Links to USACC websites pertinent to the person's position or organization may be included under the signature block.

Chapter 6 – Command Responsibilities for Freedom of Information Act (FOIA) Requests

6.1 The Freedom of Information Act (FOIA)

FOIA is a Federal release statute program in accordance with 5 United States Code (U.S.C.), and Public Law 106-554. The FOIA office implements the Office of Management and Budget (OMB), Department of Justice (DOJ), and Department of Defense (DoD) guidance regarding the FOIA and ensure the requirements of Executive Order (EO) 13392. The FOIA provides an important means through which the public can request access to records related to the Federal Government, unless the information is protected from disclosure by any of nine exemptions enacted by Congress to protect information that must be held in confidence.

6.2 The Privacy Act of 1974, as amended, 5 U.S.C. § 552a

a. The Privacy Act (PA) is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them.

b. The PA focuses on four basic guidelines:

(1) To restrict disclosure of personally identifiable records maintained by agencies.
(2) To grant individuals increased rights of access to agency records maintained on themselves.
(3) To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely or complete.
(4) To establish a code of "fair information practices" which requires agencies to comply with statutory norms for collection, maintenance, and dissemination or records.

6.3 The Request Process

a. Complete the USACC Freedom of Information Act Request form.
b. All initial requests to USACC FOIA shall be submitted via email to the FOIA/PA address usarmy.knox.usacc.mbx.hq-foia@mail.mil for processing.
c. Or Mail United States Postal Service (USPS) at:

DEPARTMENT OF THE ARMY
Headquarters, United States Army Cadet Command G6
ATTN: Freedom of Information Act Officer
"Freedom of Information Act Request"
1307 3RD AVE
FORT KNOX, KY 40121-2725
OFFICIAL BUSINESS 690

d. Request will be reviewed to meet FOIA standards.

(1) Mailing and/or email address.
(2) Reasonable description of requested records.
(3) Agreement to pay fees or request for waiver (as applicable).
(4) Verification of identity (as necessary).

6.4 Case Management

a. Request Perfected - Statutory 20 business days begins when the request is perfected. Determine components processing queues:

(1) Simple – “Easy”
(2) Complex – “Difficult”
(3) Expedited

b. A case/reference number will be assigned to the request using the Freedom of Information & Privacy Act Case Tracking System (FACTS):

(1) Request consultations and coordination’s with appropriate organization/record owners or:
(2) Request will be referred to correct organization/record owners for new initial review.

c. Send Acknowledgement letter:

(1) Date of receipt or perfected.
(2) Identify 20 day anticipated response date.
(3) Include a reference number.

d. Record Owner Inquiry/Retrieval

(1) Ask for subject matter expert (SME) point of contact (5 day suspense).
(2) Coordinate to determine if there is enough information to conduct a reasonable search.
(3) Review records, highlight portions for withholding and document harm analysis.
(4) Identify additional stakeholders (DOD consultation required).

e. The USACC FOIA officer will sanitize, redact, and provide all exemptions for FOIA per DoDM 5400.07 25JAN17, and FOIA Code of Federal Regulations (CFR) 32 § 286.12. For PA per Army Regulation 25-22, and 32 CFRs 505, to process the request.

6.5 Format

a. Electronic documents (e-documents) are the preferred method, created in .pdf using Adobe Acrobat. This simplifies the task of sending it to the recipient (email, or compacted onto a CD).

b. Hard Copy Files:

(1) Records will be converted into a digital Adobe.pdf format.
(2) If files cannot be converted to a digital format, record owners can mail/track the files via FEDEX to the following:

US ARMY CADET COMMAND G6
ATTN: Freedom of Information Act Office
BLDG 1002
204 1ST CAVALRY REGIMENT ROAD
FORT KNOX, KY 40121-2725

6.6 Supporting Documents

a. Record owners within USACC HQ Directorates, Special Staff, and Brigades will have five (5) business days to provide all responsive records intact and unaltered.

b. These electronic records will be uploaded into designated unit/origination folders located on USACC FOIA/PA SharePoint. Selected representatives in your unit/organization will have access to the secure site for uploading files (Ex. https://army.deps.mil/army/cmds/USACC-HQ/G6/FOIA/RM%205th%20Bde).

c. The U.S. Army Aviation and Missile Research Development and Engineering Center (AMRDEC) Safe Access File Exchange (SAFE) application is used to send large files to individuals which would normally be too large to send via email. There are no user accounts for SAFE - authentication is handled via email and CAC. Everyone has access to SAFE and the application is available for use by anyone. SAFE supports file sizes up to **2GB**. Instructions can be found by using the following link: https://safe.amrdec.army.mil. This tool tracks receipt of files, and is available for pickup/download up to 14 days.

6.7 Training

a. All personnel working with FOIA/PA and record owners will take the following training classes. Please provide a copy of your certification for record:

(1) Senior Executive Briefing-A short video from the Director of OIP for agency senior executives, providing a general overview of the FOIA and emphasizing the importance of their support to their agency's FOIA program. (:10 min.)

https://army.deps.mil/army/cmds/USACC-HQ/G6/FOIA/FOIA-Privacy%20Act%20Training/AG%20FOIA%20Statement%2003.11.15.mp4

(2) Dept. of Justice (DOJ) Digital FOIA e-Learning Training Modules DOJ -US001-DOJ Freedom of Information Act (FOIA) Training for Federal Employees (1:00 hrs.)

http://jko.jfcom.mil

(3) Defense Information Systems Agency (DISA) Identifying and Safeguarding Personally Identifiable Information (PII) Version 2.0 (:45 min.)

https://iatraining.disa.mil/eta/piiv2/launchPage.htm

Chapter 7 – Official Mail

a. Each Brigade will assign a primary and alternate Official Mail Manager (OMM) who is responsible for submitting reports of postal expenditures for all official mail sent from the Brigade HQ in accordance with AR 25-51. Reports must be submitted in the Automated Military Postal System (AMPS). The deadline for 1st and 2nd Quarter FY expenditures is 15 April and the deadline for 3rd and 4th Quarter FY expenditures is 15 October.

b. Each Brigade will create an Official Mail Manager User (OMM User) account in the AMPS system for assigned primary and alternate Brigade postal officer. These accounts are coordinated through the G6 and require a DD 2875 form for system access to AMPS and an appointment memorandum assigning postal reporting responsibilities to the designated postal officers.

c. All SROTC official mail expenditures are reported in the Cadet Command Information Management Module (CCIMM) using the postal reporting module. OMMs will consolidate their associated SROTC and Brigade HQ expenditures to report in the AMPS system. SROTC Programs are only required to report postal expenditures that are paid for by government funds (i.e., Brigades are not required to report postage expenditures covered by the university on behalf of the ROTC Program).

APPENDIX A – References

Section I – Referenced Publications

a. DoD Manual 5200.01 – V 3.0 (DoD Information Security Program: Protection of Classified Information), 24 Feb 12.

b. DoD Directive 8570.1 (Information Assurance Training, Certification, and Workforce Management), 23 Apr 07.

c. BBP 03-PE-O-0002 – V 1.7 (Reuse of Army Computer Hard Drives), 2 Jun 09.

d. Army Regulation 25-1 (Army Information Technology), 25 Jun 13.

e. Army Regulation 25-2 (Information Assurance), 23 Mar 09.

f. Army Regulation 25-400-2 (The Army Records Information Management System (ARIMS)), 2 Oct 07.

g. Army Regulation 71-32 (Force Development and Documentation), 1 Aug 13

h. Army Regulation 380-5 (Information Security), 29 Sep 00.

i. DA PAM 25-1-1 (Army Information Technology Implementation Instructions), 25 Jun 13.

j. TRADOC Supplement 1 to AR 25-2 (Information Assurance), 14 Sep 10.

k. Memorandum, DoD CIO, 03 Jul 07, subject: Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media.

l. Army Chief Information Officer (COI)/G6 Memorandum, 17 Dec 12, subject: Army Policy Requiring the Use of Next-Generation (NextGen) Department of Defense (DoD) Handheld Wireless Enterprise Blanket Purchase Agreements (BPAs) to Identify and Eliminate Devices Based on Usage.

m. Memorandum, SAIS-CB, 25 Jul 12, subject: Changes to the Title, Responsibilities and Certification Requirements for Information Assurance Security Officers (IASO) Extension.

Section II – Prescribed Publications

USACC Incident Handling Plan

Information Technology Equipment Authorization Spreadsheet

USACC Media Sanitation and Destruction SOP

Information Technology Enterprise Change Management SOP

APPENDIX B – Rescinded IT Policy Letters

a. IT Policy 01 - Command-wide Standard for Electronic Mail (E-Mail)

b. IT Policy 02 - Use of Government Furnished Cellular Devices

c. IT Policy 03 - Control of Removable Media

d. IT Policy 04 - Managing and Protecting Mobile-Portable Electronic Devices

e. IT Policy 05 - Protection of Information Technology Equipment and Personally Identifiable Information

f. IT Policy 06 - User Responsibilities to Ensure Information Assurance

g. IT Policy 07 - Senior Reserve Officers' Training Corps Program Information Assurance Support Officer

h. IT Policy 08 - Sensitive and Classified Information Spillage

i. IT Policy 09 - Requirements for Wireless Technologies

j. IT Policy 10 - Protecting Data-At-Rest

k. IT Policy 11 - Virtual Private Network Usage

l. IT Policy 12 - Protection of Classified Information

m. IT Policy 13 - Protection of Controlled Unclassified Information

n. IT Policy 14 - Common Access Card and Public Key Infrastructure Usage and Protection

o. IT Policy 15 - Authorized Use of Telecommunications Systems

p. IT Policy 16 - Consent to Monitoring

q. IT Policy 19 – Use of Printers, Copying, and Multi-Function Devices within USACC

GLOSSARY

Section I – Acronyms and Abbreviations

AO
Action Officer

ATCTS
Army Training and Certification Tracking System

AUP
Acceptable Use Policy

BBP
Best Business Practices

BOIP
Basis of Issue Plan

C4IM
Command, Control, Communications, Computers, and Information Management

CAB
Change Advisory Board

CCB
Change Control Board

CCIMM
Cadet Command Information Management Module

CNACI
Child Care National Agency Check with Inquiries

DAR
Data at Rest

DISA
Defense Information Systems Agency

DoD
Department of Defense

DoLD-E
Directorate of Leader Development and Education

ECM
Enterprise Change Management

HDD
Hard Disk Drive

IA
Information Assurance

IA BBP
Information Assurance Better Business Practice

IASO
Information Assurance Security Officer

IM
Information Management

IMO
Information Management Officer

IS
Information System

IT
Information Technology

ITEPS
Information Technology Equipment, Products, and Services

NAC
National Agency Check

NACI
National Agency Check and Inquiries

PED
Portable Electronic Device

PII
Personally Identifiable Information

PMID
Project Management Integration Division

PST
Personal Storage Table

RFC
Request for Change

RMID
Recruiting, Marketing and Incentives Directorate

TDA
Table of Distribution and Allowances

UPT
Universal Purge Tool

VPN
Virtual Private Network

Section II – Terms

This section contains no entries.