

**BY ORDER OF THE COMMANDER,
UNITED STATES AIR FORCES IN
EUROPE (USAFE)**

AIR FORCE MANUAL 33-363



**UNITED STATES AIR FORCES IN EUROPE
Supplement**

25 NOVEMBER 2008

Certified Current on 14 August 2015
Communications and Information

MANAGEMENT OF RECORDS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at www.e-publishing.af.mil for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AFCA/EASM

Certified by: AFCA/EAS
(Mr. Bernard J. Honsberger)

Supersedes: AFMAN37-123_USAFESUP1,
7 April 2007

Pages: 13

AFMAN 33-363, 1 March 2008, is supplemented as follows: This supplement applies to all United States Air Forces in Europe (USAFE) units. This supplement implements tasks and responsibilities for storing electronic records on main operating base and geographically separated unit shared storage servers. It establishes how units will manage electronic records in that environment and provides guidance for storage of official electronic records and personal working files using a shared network drive. It does not apply to Air National Guard (ANG) or Air Force Reserve Command (AFRC) units. Coordinate proposed supplements with the Command Records Manager (AFCA/EASM), 203 W. Losey St., Rm. 1100, Scott AFB, IL 62225 or email afca.easm.rm@us.af.mil prior to publication. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located in Air Force Records Information Management System (AFRIMS) at Air Force (AF) Portal: <https://www.my.af.mil/gcss-af61a/afrims/afrims/rims.cfm>

SUMMARY OF CHANGES

Supplemented publication and numbering updated. AFRIMS section deleted.

6.22.1. (Added) Managing and Storing Electronic Records on Shared Storage Servers.

6.22.1.1. (Added) Overview and Objectives. The Chief of Staff of the Air Force and

Secretary of the Air Force directed consolidation of network servers to dramatically improve operations and significantly reduce Air Force information technology total cost of ownership. In USAFE, main operating bases (MOB) and geographically separated units (GSU) will be supported by consolidated network storage servers to carry out this directive. At locations where a Storage Area Network (SAN) is not available or feasible, base-level communications squadrons must obtain and designate a drive as the shared electronic storage space for their installation's official electronic records. This dedicated electronic storage space should function as a central electronic repository for filing official records.

6.22.1.1.1. (Added) The shared storage server provides a single repository for information and an effective electronic file and record management structure for users. The Network Operations and Security Center (NOSC) provides storage space to each installation, the installation Communications Squadrons maintain the storage space for their installation, and data owners are responsible for managing their stored information.

6.22.1.1.2. (Added) The shared storage servers provide storage space for official electronic records, official working files, and non-official personal working files. An official electronic record is a computer generated file that documents the transaction of official Air Force business. Electronic personal working files consist of work-related diaries, journals, personal calendars, appointment schedules, etc., and exist for personal use to assist in conducting (but not transacting) Air Force business. The official record is complete with attachments or related data when filed. Once the electronic document becomes the official record it will not be changed, modified, or altered. To preserve the integrity of official records save the official file copy as a read-only record.

6.22.1.2. (Added) Drive Structure. Each shared storage server will be divided into four separate storage drives which segregate different types of data as follows:

6.22.1.2.1. (Added) Official ("O:" drive) is the network resource used to store official records. The directory structure is based on organization and office symbols which maintain official records and have an approved file plan in AFRIMS (**Figure 6.5. (Added)**). File retention is determined by the Air Force Records Disposition Schedule (RDS) located in AFRIMS on the Air Force Portal. Each office of record folder on the "O:" drive will contain the following folders:

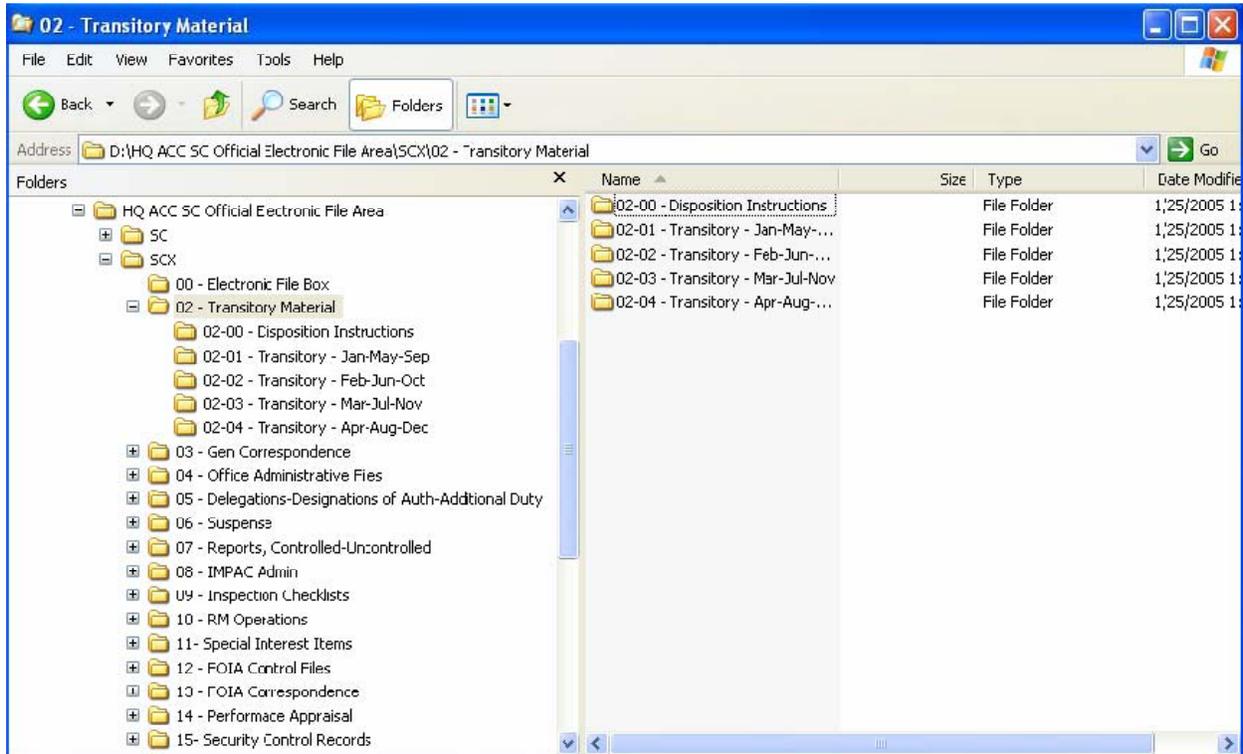
6.22.1.2.1.1. (Added) 00-Electronic File Box-Contains official records that the end user drags and drops from a shared drive, local hard-drive, or Outlook (if they do not know which file on the e-file plan to place it) for filing by the Records Custodian (RC).

6.22.1.2.1.2. (Added) 01- File Maintenance and Disposition (Media Neutral)- Contains a copy of the approved file plan exported from AFRIMS. It is a record keeping requirement to store the official file plan with the file folders it governs.

6.22.1.2.1.3. (Added) All folders, numbered as listed on the approved file plan, where electronic official files exist. Each folder will contain a sub-folder named XX-00 (where XX is the file number from the approved AFRIMS file plan) containing the applicable table and rule extracted from the RDS. Individuals will file directly to the applicable e-file on the file plan unless they do not know which one to file to and then they will place the file in the 00-Electronic File Box for the RC to file.

6.22.1.2.1.4. (Added) Inactive Files Folder-Contains records that have met cutoff (Fiscal Year (FY) or Calendar Year (CY)) but not met their retention period according to Air Force RDS located in AFRIMS. These records will be retained in the inactive folder by year group until they are either eligible for destruction or removal to off-line storage in accordance with the Air Force (AF) RDS until eligible to be transferred to the appropriate National Records Center for storage.

Figure 6.5. (Added) The Electronic Record “O:” Drive Structure.



6.22.1.2.2. (Added) Organizational Shared (“S:” drive) is the network resource provided for storage of organizational data needing to be shared base-wide (enterprise-wide in the future). There is a single “S:” drive and all base users will share this common path. Each organization will have a folder on the organizational drive with subfolders to the office level. Organizations may use the “S:” drive to maintain or share tasks-in-progress and as a temporary holding bin for official, nonrecord information (i.e. promotion/ retirement invites, barbecue flyers, etc.). Additionally, the “S:” drive will have an Official Multimedia folder containing official multimedia files. Recommend each office set the top folders as: Templates, Reference, Working, and Collaboration for organizational purposes. The Network Control Center (NCC), Client Support Administrators (CSA), and end users will be responsible for maintaining this area. The “S:” drive folders must be, by default, accessible to all authenticated base personnel. This is to meet the requirements for inter-organization data sharing. Due to access availability, do not file any Privacy Act, Personal Health Information (PHI) and Confidential Data (HIPPA) or other sensitive information on “S:” drive.

6.22.1.2.2.1. (Added) The “S:” drive storage area is not for official records.

Once a task/document is completed or an event has passed, the information owner will remove it from the "S:" drive, and either properly file it into the appropriate file on the e-file plan or the 00-Electronic File Box (if they do not know the appropriate file) on "O:" drive, or dispose of it accordingly. To assist in preventing storage limits from being exceeded based on allocation guidelines established by the NOSC, files that have not been modified for more than 365 days and unauthorized files (paragraph **6.22.1.3.4.** (Added)) will be identified weekly by the NCC and provided to the organization for disposition.

6.22.1.2.2.2. (Added) Set the file attribute to "Read Only" when saving files to the "S:" drive that must be shared but also must remain intact.

6.22.1.2.3. (Added) Office-Restricted ("R:" drive) is the network resource provided to share office-specific information. Access to the "R:" drive is limited to members assigned to the office. Offices may use the "R:" drive to maintain working or reference files that only pertain to the office. Working data files such as recall rosters, leave schedules, temporary duty (TDY) schedules, duty schedules, and internal office procedures may reside on the "R:" drive; the official copies need to be filed on the "O" drive. Do not store official records on the "R:" drive. The NCC, CSAs, and end users will be responsible for maintaining this area. To prevent storage limits from being exceeded based on allocation guidelines established by the NOSC, files that have not been modified in more than 365 days and unauthorized file (paragraph **6.22.1.3.4.** (Added)) will be identified weekly by the NCC and provided to the organization for proper disposition.

6.22.1.2.4. (Added) User ("U:" drive) is the network resource provided for users to store personal information (electronic work related personal papers and background materials), non-record information, personal working files or copies of official tasks in progress. AFI 33-364, *Records Disposition - Procedures and Responsibilities*, governs the maintenance, storage, and disposition of electronic personal records. Each personal folder on the "U:" drive will utilize the naming convention firstname.lastname (i.e., john.doe) for that individual. All end-users will have a personal folder on the "U:" drive. Users will not store official files on the "U:" drive. Users are responsible for maintaining the file permissions for the content within their personal workspace and ensuring that their storage utilization does not exceed their quota limitation established by the NOSC.

6.22.1.3. (Added) File Restrictions. The following file types will not be stored on the "O:", "S:", "R:", or "U:" drives:

6.22.1.3.1. (Added) Permanent backups and archives of desktop and portable computer hard drives. Files of this type will be deleted by the NCC/CSA (for "R:", "S:", and "U:" drives) or Base Records Manager (BRM)/ Functional Area Records Manager (FARM)/ RC (for "O:" drive) 10 work days after creation. Desktop and portable computer data is commonly copied to network storage during personnel moves, computer replacement or upgrades. User data, such as documents may be copied to network storage ("U:" drive); however, entire hard disks (program files and Windows installation directory) will not be copied to network storage.

6.22.1.3.2. (Added) Libraries. Publications and forms that are available on official publication web sites will be downloaded as needed from official sources and will not be

duplicated on network storage.

6.22.1.3.3. (Added) Software installation files. Where required, these files will be hosted by the communications squadron in a storage area that does not consume backup resources. Recovery to this area will be from the original installation media.

6.22.1.3.4. (Added) Personal data files including *.wav, *.jpg, *.mp3, *.mpeg, *.avi, *.pst, *.tmp, *.exe, *.ost, *.oab, *.wmv, *.mov, *.tif, *.bin, *.iso, *.nrg, *.vob, *.m4a, *.dll, *.sys, *.ocx, *.vbx, *.vxd, *.drv, *.scr, *.cpl, *.gho, *.msc and any other files extensions of these types. The only exception to this is *.pst files which may be stored on the "U:" drive and must adhere to applicable guidance. The NOSC will implement filters to the organization/office folders of the "R:" and "S:" drives (with the exception of the "Multimedia" folder in the organizations root directory) to prevent additional files of these types from being saved to these shared drives. The NCC will make recommendations to the NOSC to add additional file extensions to the command unauthorized files list. The NOSC will provide any additions to this list via Notice to Airmen (NOTAM).

6.22.1.3.5. (Added) Electronic Records Management (ERM). The "R:" and "S:" drives have been established for ERM working file storage. The only files authorized on the "R:" and "S:" drives are those having a requirement to be collaborated on by more than one user. As a rule, these will be "living" documents that are accessed or updated on a regular basis. The "O:" drive is for official records storage only. The shared drives "R:", "S:" and "U:" are not for archiving personal files.

6.22.1.4. (Added) Roles and Responsibilities. The following paragraphs identify additional roles and responsibilities required for effective management of electronic records on shared storage servers.

6.22.1.4.1. (Added) AFCA/EASM provides guidance and policy on file cleanup of shared drives and records management.

6.22.1.4.2. (Added) Commanders and Directors will ensure individuals appointed as BRM, FARM, Chief of Office of Record (COR), and RC receive appropriate training within 90 days of appointment.

6.22.1.4.3. (Added) Network Operations and Security Center (NOSC) will:

6.22.1.4.3.1. (Added) Manage and configure shared storage servers to provide the four shared network drives.

6.22.1.4.3.2. (Added) Work with the base NCC to establish sizing of storage server resources.

6.22.1.4.3.3. (Added) Work with the base NCC to establish and enforce allocation limitations on the four shared network drives, based on available storage resources.

6.22.1.4.3.4. (Added) Ensure regular backups of the shared network drives. Ensuring daily backups of the "O:" drive are maintained a minimum of 90 days and maximum of 120 days for restoration purposes. Maintain "R:", "S:", and "U:" drive backups, up to 30 days, based on availability of resources.

6.22.1.4.3.5. (Added) Apply filters to the "R:" and "S:" drives to preclude

introduction of additional unauthorized file type to these shared drives. (**Exception:** the “Multimedia” folder in each units root directory.)

6.22.1.4.4. (Added) Network Control Centers (NCC) will:

6.22.1.4.4.1. (Added) Establish and maintain the organizational structuring of data on the “R:” and “S:” drive using the current organizational office symbols starting at headquarters and squadron two-digit levels (i.e., Commander 52 Communications Squadron (52 CS/CC), USAFE Director of Staff (USAFE/DS)) and “U:” drive using network login naming convention of firstname.lastname.

6.22.1.4.4.2. (Added) Assist the BRM in establishing and maintaining the organizational structure of data on the “O:” drive. Office folders on this drive will be based on office of record loaded in AFRIMS (units with approved file plans).

6.22.1.4.4.3. (Added) Assist with assigning permissions as outlined in **Table 6.2. (Added)**. NCC will not assign FARM/RC permissions to the “O:” drive without prior approval and coordination from the BRM.

Table 6.2. (Added) Shared Storage Permissions.

Shared Storage Server Permissions Matrix							
Storage Area	NOSC/ NCC	CSA	BRM	FARM	COR	RC	End-User
O:\	F		F				
Org Folders	F	F	F	R/W/M	R/W/M	F	R/W
00- Electronic File Box	F F		F	R		F	R/W
Inactive Files	F	F	F	R/W/M	R	F	R
Files	F	F	F	R/W/M	R	F	R
S:\	F	F	R	R	R	R/W/M	R
Org Folders	F	F	R	R	R/W/M	R/W/M	C
R:\	F	F	R	R	R	R/W/M	R
Org Folders	F	F	R	R/W/M R/	W/M R/	W/M	C
U:\	F	F					
End-user Folders	F						C
LEGEND							

NOSC/NCC: Network Operations and Security Center/Network Control Center	CSA: Client Support Administrator
BRM: Base Records Manager	FARM: Functional Area Records Manager
COR: Chief of Office of Record	RC: Records Custodian
F: Full	C: Change Access (R/W/M/D)
R: Read	W: Write
M: Modify	D: Delete

6.22.1.4.4.4. (Added) Enforce allocation limitations on the four shared network drives. Monitor status of backups of the shared network drives. Ensuring daily backups of the “O:” drive are maintained a minimum of 90 days and maximum of 120 days for restoration purposes. Maintain “R:”, “S:”, and “U:” drive backups, up to 30 days, based on available resources.

6.22.1.4.4.5. (Added) Process and coordinate storage allocation increase requests.

6.22.1.4.4.6. (Added) Scan for and notify Squadron Commander of potentially unauthorized files and files not modified within the past 365 days stored on the “R:” and “S:” drives on a weekly basis.

6.22.1.4.5. (Added) Command Records Manager will:

6.22.1.4.5.1. (Added) Coordinate with BRMs to facilitate local implementation of base-level training.

6.22.1.4.6. (Added) Base Record Managers (BRM) will:

6.22.1.4.6.1. (Added) Serve as the installation focal point for electronic records management and information migrated and stored on the “O:” drive.

6.22.1.4.6.2. (Added) Ensure individuals appointed as a FARM, COR, or RC complete the appropriate level of Records Management (RM) Computer Based Training (CBT) prior to creation of an AFRIMS account and assigning permission for access to the “O:” drive.

6.22.1.4.6.3. (Added) Work with the NCC to assign permissions.

6.22.1.4.6.4. (Added) Accomplish weekly searches of the “O:” drive for unauthorized files. Provide listing of files to the FARM to disseminate to the COR/RC for removal.

6.22.1.4.6.5. (Added) Review ERM progress during Staff Assistance Visits (SAV).

6.22.1.4.6.6. (Added) Coordinate on storage allocation increase requests for the “O:” drive.

6.22.1.4.6.7. (Added) Accomplish Records Management CBT level 1, 2, and 3

within 90 days of appointment.

6.22.1.4.7. (Added) Functional Area Record Managers (FARM) will:

6.22.1.4.7.1. (Added) Assist office of records within their organization or functional area with setting up their electronic records.

6.22.1.4.7.2. (Added) Provide guidance/oversight on ERM processes and assists RCs with populating, migrating, and creating file plan structure on the "O:" drive.

6.22.1.4.7.3. (Added) Provide organizational CSAs with an accurate organizational address listing of offices of record requiring permissions to be set.

6.22.1.4.7.4. (Added) Ensure CORs and RCs accomplish Records Management CBT level 1 and level 2, and annual refresher training.

6.22.1.4.7.5. (Added) Notify CSAs of personnel who require immediate termination of access to Enterprise Storage Network (ESN) drives (Permanent Change of Station (PCS), Article 32 or other Uniform Code of Military Justice (UCMJ) action, etc).

6.22.1.4.7.6. (Added) Accomplish Records Management CBT levels 1, 2 and 3 as well as any local training required by BRM within 90 days of appointment. All training will be accomplished prior to gaining access to AFRIMS or the "O:" drive. Accomplish annual refresher records management training.

6.22.1.4.8. (Added) Client Support Administrators (CSA) will:

6.22.1.4.8.1. (Added) Using Directory and Resource Administrator (DRA), assign personnel to folder groups. Each folder group has permissions (i.e., read, write, modify) assigned. Additions and deletions of individuals from organizational address listings will be received from the FARM, COR or RCs.

6.22.1.4.8.2. (Added) Provide new office of record information to NCC for creation of appropriate subfolders.

6.22.1.4.8.3. (Added) Establish and maintain office of record organizational address listing under their purview. (**Note:** CSAs will only update listings upon request from FARMS, COR, or RCs.)

6.22.1.4.8.4. (Added) Act as organizational custodians of the "R:", "S:", and "U:" drives.

6.22.1.4.8.5. (Added) Review and coordinates on storage capacity increase requests for the "R:" and "S:" drives.

6.22.1.4.9. (Added) Chief of Office of Record (COR): The COR is responsible for official electronic records created by his or her office. The COR will:

6.22.1.4.9.1. (Added) Ensure vital records are identified for protection during emergencies, contingencies, and natural disasters according to requirements outlined in AFI 33-364, *Records Disposition - Procedures and Responsibilities*.

6.22.1.4.9.2. (Added) Work with the RC to create a file plan and identify records maintained electronically within 90 days of establishment of an office of record.

6.22.1.4.9.3. (Added) Ensure the file plan includes an unclassified description of all

electronic classified records maintained by the office of record. DO NOT FILE CLASSIFIED RECORDS ON AN UNCLASSIFIED STORAGE SERVER.

6.22.1.4.9.4. (Added) Appoint an RC and ensure the RC accomplishes level 1 and 2 RM CBT within 90 days.

6.22.1.4.9.5. (Added) Ensure office personnel are briefed on electronic filing structure and process to ensure they understand electronic filing requirements.

6.22.1.4.9.6. (Added) Brief the RC on the functional mission of the office of record that the records support. Ensure RC understands the requirement to protect personal and For Official Use Only (FOUO) information maintained on the storage servers in accordance with AFI 33-322, *Records Management Program* and the *Privacy Act of 1974*.

6.22.1.4.9.7. (Added) Ensure corrective action is taken on discrepancies noted during records management SAVs.

6.22.1.4.9.8. (Added) Coordinate on requests for storage allocation increase requests for the "O:" drive.

6.22.1.4.9.9. (Added) Accomplish Records Management CBT level 1 and 2 within 60 days of appointment. Accomplish annual refresher records management training.

6.22.1.4.9.10. (Added) Ensure the RC is reviewing "R:" and "S:" drive files to identify official records and moving them to the "O:" Drive.

6.22.1.4.10. (Added) Records Custodians (RC) will:

6.22.1.4.10.1. (Added) Build the Electronic File Plan structure on the "O:" drive in accordance with an approved AFRIMS file plan.

6.22.1.4.10.2. (Added) Coordinate office file plan and submit the file plan in AFRIMS to the BRM for review and approval.

6.22.1.4.10.3. (Added) Ensure individuals in their office of record are given the file permissions on storage devices commensurate with their responsibilities.

6.22.1.4.10.4. (Added) Contact FARMS if individual permissions are required to be set.

6.22.1.4.10.5. (Added) Maintain the electronic file location using the same principles applied to office paper files, including applying tables and rules, end-of-year close out (Fiscal and Calendar), transferring records to the inactive files area, and destroying records no longer needed according to the Air Force RDS located in AFRIMS (<https://www.my.af.mil/gcss-af61a/afirms/afirms/rims.cfm>) on the Air Force Portal.

6.22.1.4.10.6. (Added) Request limited file-access permissions for members of the office of record, if required.

6.22.1.4.10.7. (Added) Evaluate the information their office has stored on the local file server and move official records to the proper file folder in the electronic file plan.

6.22.1.4.10.8. (Added) Move information from the 00-Electronic File Box to the proper file folder in the electronic file plan on the "O:" drive as necessary.

- 6.22.1.4.10.9. (Added) Complete Records Management CBT levels 1 and 2 as well as any locally required training within 90 days of appointment. All training will be completed prior to gaining access to the “O:” drive or AFRIMS. Accomplish annual refresher records management training.
- 6.22.1.4.10.10. (Added) Transfer electronic active records to “O:” drive inactive folder at end of FY/CY according to disposition of the records.
- 6.22.1.4.10.11. (Added) Notify the organization CSA of changes to the office of record organizational address listing.
- 6.22.1.4.10.12. (Added) Ensure personnel assigned to the office of record are members of the organizational address listing.
- 6.22.1.4.10.13. (Added) Initiate storage allocation increase requests for the “O:” drive.
- 6.22.1.4.11. (Added) End-Users:
- 6.22.1.4.11.1. (Added) Accomplish Information Protection CBT annually.
- 6.22.1.4.11.2. (Added) Determine which electronic records are official and manage those in accordance with Federal Laws and Air Force guidance.
- 6.22.1.4.11.3. (Added) Ensure they have the proper permissions to storage devices, and if they do not, work with their RC for “O:” drive or CSA for “R:” or “S:” drives to gain the permissions authorized for their work center.
- 6.22.1.4.11.4. (Added) Sanitize their personal files to ensure only up-to-date, pertinent information is stored.
- 6.22.1.4.11.5. (Added) Place official records in office of record 00-Electronic File Box on the “O:” drive. If record is sensitive, consider password-protecting the file to prevent unauthorized access.
- 6.22.1.4.11.6. (Added) End-users will not have the capability or functions to remove, replace, or delete official records. Notify the RC who will remove official record from the “O:” drive.
- 6.22.1.5. (Added) Shared Storage Permissions. The following paragraphs describe individual permissions for shared storage directories (**Table 6.2. (Added)**).
- 6.22.1.5.1. (Added) CSAs have full access to only the organizational storage drives and folders of the 2-letter organization for which they work. For example, a 52 Operations Group (OG) CSA won’t be able to access 52 Logistics Group (LG) storage drives or folders.
- 6.22.1.5.2. (Added) FARM permissions apply to the organizational folders for the offices they oversee.
- 6.22.1.5.3. (Added) Permissions only apply to the organizational folders for an office of record where the individual works. For example, on the “O:” drive, a COR, RC, and end-user assigned to History Office (86 AW/HO) will only have permissions to 86 AW/HO folders. Also, folders and, or files on the “O:” drive that contain sensitive information (Privacy Act, FOUO, etc.) will only be accessible by the RC, COR, and end-user who are

Office of Primary Responsibilities (OPR) for the information. Consider password-protecting extremely sensitive files to prevent unauthorized access. On the “S:” and “R:” drives, “modify” access permissions apply from the office symbol-level down. On the “U:” drive access permissions apply at the folder-level.

6.22.1.5.4. (Added) Change access is Read, Write, Modify, and Delete (R/W/M/D). The only individuals with full access are NOSC/NCC system administrators and organizational CSAs for all drives, Records Custodians and Base Records Managers for the “O:” drive, and end-user for individual “U:” drive.

6.22.1.5.5. (Added) Permissions to the file structure on the “O:”, “R:”, and “S:” drives are only granted via office symbol groups. No individual accounts should be listed on the file structure.

6.22.1.6. (Added) Business Rules:

6.22.1.6.1. (Added) Maintain electronic records with a retention period of 10 years or less in the electronic files area (Inactive area) on the “O:” drive. A backup of inactive file directories must be accomplished by the office of record at the end of each calendar year. Electronic records with a retention period of greater than 10 years must be staged and sent to the FARM/BRM with a completed SF Form 135, *Records Transmittal and Receipt*.

6.22.1.6.2. (Added) Files to be sent to staging or transferred to National Archives and Records Administration (NARA) must be saved in one of the following formats:

6.22.1.6.2.1. (Added) Textual records (of or pertaining to text) - plain American Standard Code for Information Interchange (ASCII) or in Portable Document Format (PDF) format or scanned images.

6.22.1.6.2.2. (Added) Scanned images of textual records - the preferred formats are Tagged Image File Format (TIFF) and Portable Network Graphics (PNG). Graphics Interchange Format (GIF) and, Basic Image Interchange Format (BIIF) are also acceptable.

6.22.1.6.2.3. (Added) Data files and databases - convert tables to files with fixed-length fields or fields defined by delimiters.

6.22.1.6.2.4. (Added) Digital geospatial data - Spatial Data Transfer Standard (SDTS) or Geography Markup Language (GML).

6.22.1.6.2.5. (Added) Digital photographic records - Tagged Image File Format (TIFF), JPEG File Interchange Format (JFIF) and Joint Photographic Experts Group (JPEG) are also acceptable.

6.22.1.6.2.6. (Added) Web records - Hypertext Markup Language (HTML) and other formats such as TIFF or PDF that either are embedded in the HTML or referenced by it.

6.22.1.6.3. (Added) End-users will drag and drop E-mails into the appropriate file on the e-file plan or the 00-Electronic File Box (if they do not know the appropriate file) on “O:” drive. Attachments are saved with the basic message as a combined, single record, preserving the integrity of the relationship between the component parts, while allowing

retrieval of the complete item once it has been filed.

6.22.1.6.4. (Added) All work centers with a requirement to file official records on the "O:" drive will be an office of record, and must have an approved AFRIMS file plan prior to gaining access to the "O:" drive.

6.22.1.6.5. (Added) Maintain as much information electronically as possible (E-mail, correspondence, presentations, etc.); however if a signature is required by statute or law (as in legal or financial purposes), maintain the paper copy as the official record.

6.22.1.6.6. (Added) Vital record categories or series must be identified by placing a "V" or "Vital" immediately following the electronic file folder/directory title. If the folder/directory contains records not considered "Vital," identify each "Vital" document by placing a "V" or "Vital" immediately following the document title.

6.22.1.6.7. (Added) If it is necessary to integrate official electronic records with paper records, one or the other must contain a complete official record copy. The COR, RC, and OPR must determine which version (electronic or paper) contains the official records and ensure the official record is managed according to records management instructions.

6.22.1.6.8. (Added) This section outlines the process for requesting an increase in allocated space for each of the four shared storage drives.

6.22.1.6.8.1. (Added) "O:" drive - The section or unit will contact their COR to review stored data for compliance with ERM standards. If data stored is compliant, the COR will forward the request through the BRM to the NCC. The base NCC will coordinate with the NOSC to implement.

6.22.1.6.8.2. (Added) "R:" and "S:" drives - The organization will contact the CSA who will review stored data. If stored files are compliant with business rules and regulations they coordinate with the NCC and NOSC to increase storage based upon available resources and requirements.

6.22.1.6.8.3. (Added) "U:" drive - The NCC will maintain a tiered stored allocation standard to give Commanders flexibility to assign space up to a set limit. Any further increases will be reviewed and approved by the NOSC.

6.22.1.6.9. (Added) Do not file encrypted E-mails on the "O:" drive. The recipient must remove the encryption prior to filing. To accomplish this, the recipient must forward the email to themselves as an un-encrypted email.

6.28. (USAFE) Forms Adopted: SF 311, *Records Transmittal and Receipt*.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Privacy Act of 1974

UCMJ Article 32, *Uniform Code of Military Justice – Investigation*

Abbreviations and Acronyms

CBT—Computer Based Training

CY—Calendar Year

FY—Fiscal Year

HTML—Hypertext Markup Language

JPEG—Joint Photographic Expert Group

NOSC—Network Operations and Security Center

TIFF—Tagged Image File Format

USAFE—United States Air Forces in Europe

DOUGLAS W. GRAY, YC-03, DAF
Director, Architectures & Analysis