

1 December 2011

Information Management

Army in Europe Enterprise Content Management

For the Commander:

JAMES C. BOOZER, SR.
Major General, GS
Chief of Staff

Official:



DWAYNE J. VIERGUTZ
Chief, Army in Europe
Document Management

Summary. This regulation prescribes policy and procedures for enterprise content management in the Army in Europe.

Applicability. This regulation applies to all organizations with accounts connected to Army in Europe information networks and that use these networks to store, process, or share information within the Army in Europe domain.

Supplementation. Organizations will not supplement this regulation without USAREUR G3 (AEAGC-KM) approval.

Suggested Improvements. The proponent of this regulation is the USAREUR G3 (AEAGC-KM, DSN 370-7153). Users may suggest improvements to this regulation by sending DA Form 2028 to the USAREUR G3 (AEAGC-KM), Unit 29351, APO AE 09014-9351.

CONTENTS

1. Purpose
2. References
3. Explanation of Abbreviations
4. Responsibilities
5. Enterprise Content Management
6. Record Retention Requirements
7. Naming Conventions and Version Control
8. Portal Branding Requirements
9. Metadata
10. Data Retention and Archiving

Table

1. Portal Branding Requirements

Figures

1. Memorandum of Understanding Between the Knowledge Management Branch, Office of the Deputy Chief of Staff, G3, HQ USAREUR, and HQ USAREUR Staff and Organizational Content Managers
2. Sample Appointment Memorandum for a SharePoint Site Collection Administrator

Glossary

1. PURPOSE

This regulation establishes policy and procedures for performing enterprise content management (ECM) in the Army in Europe and provides USAREUR staff and organizational content managers (CMs) with best business practices (BBPs) for storing data.

2. REFERENCES

a. Publications.

- (1) AR 25-1, Army Knowledge Management and Information Technology.
- (2) AR 25-400-2, The Army Records Information Management System (ARIMS).
- (3) DA Pamphlet 25-403, Guide to Recordkeeping in the Army.
- (4) AE Regulation 25-71, Website Administration.
- (5) DOD Web Site Administration Policies & Procedures (http://www.defense.gov/webmasters/policy/dod_web_policy_12071998_with_amendments_and_corrections.aspx).

b. Form. DA Form 2028, Recommended Changes to Publications and Blank Forms.

3. EXPLANATION OF ABBREVIATIONS

The glossary defines abbreviations.

4. RESPONSIBILITIES

a. Knowledge Management (KM) Branch, Office of the Deputy Chief of Staff, G3, HQ USAREUR. The KM Branch is responsible for—

- (1) Managing the Army in Europe ECM Program, which is designed to help individuals and organizations effectively perform content-management duties.
- (2) Preparing a memorandum of understanding defining the roles and responsibilities of the KM staff and content managers (fig 1).

b. Senior Leaders. Senior leaders, including directorate and division chiefs and commanders of major subordinate commands (MSCs), will appoint as a minimum one CM for their units and a SharePoint site collection administrator if applicable at their level (fig 2).

c. Organizational CMs. Organizational CMs will—

(1) Train their organization’s personnel and provide guidance on ECM policy, procedures, and responsibilities.

(2) Conduct quarterly reviews of files in all data stores, hardcopy records, and metadata for compliance with the policy and procedures in this regulation.

(3) Ensure the use of common naming conventions and metadata within their organizations. If file names provide insufficient information, CMs will contact the document owners for correction and provide training on naming conventions and version control, if necessary.

(4) Be responsible for uploading content to publicly accessible websites.

5. ENTERPRISE CONTENT MANAGEMENT

a. Definition. Content management comprises technologies and processes that support the collection, management, and publication of information in any format or medium. This information is typically referred to as content or digital content. Digital content may take the form of text files, multimedia files (such as audio or video files), or any other type of file that is subject to a content life cycle requiring management. ECM includes—

(1) The strategies, methods, and tools used to capture, manage, store, preserve, and deliver content and documents related to organizational processes. ECM covers the management of information within the entire scope of an enterprise, whether that information is a paper document, an electronic file, a database print stream, or an e-mail message.

(2) Document management, web-content management, search and collaboration processes, records management, digital-asset management, workflow management, data-capturing, and data-scanning. The primary intent of ECM is to manage the life cycle of information from creation through archiving to disposal.

b. Purpose of ECM. As information grows in quantity, variety, and complexity, the types of sources that generate information also continue to grow. With the amount of data being generated, standards on how to create and save documents are essential to ensuring that documents can be logically stored and easily retrieved. ECM provides these standards. If data is not managed, data-storage devices become “digital landfills” that are full of unused, aging, nonauthoritative, and sometimes misleading data. The purpose of ECM is to—

(1) Ensure the four basic attributes of ECM apply to all stored data (d below).

(2) Ensure existing data is not recreated.

(3) Prevent data losses.

c. Requirements of an Effective ECM Program. All individuals who create documents are CMs and must apply the principles of ECM to their own documents. All content intended for use outside of the office or directorate, such as content that will be placed on the EUR SharePoint Portal, a shared drive, or a website, must comply with the content management principles in this regulation. Individual CMs are responsible for managing content by—

(1) Periodically reviewing files for archiving and deletion.

(2) Familiarizing themselves with file-retention requirements (AR 25-400-2).

(3) Adding metadata to documents in accordance with their organization's metadata strategy (para 9).

(4) Using standard naming conventions for all files.

(5) Archiving inactive records that must be retained and deleting those that do not have any retention requirements. Most documents should be discarded after 6 years (AR 25-400-2).

(6) Periodically reviewing file content to maintain usefulness to the organization.

(7) Consulting with other people in their organizations about archiving completed projects, organizing files, and deleting drafts.

(8) Providing guidance to their replacements (if known) before leaving the organization. The guidance should explain ECM standards the replacement will need to know and apply as a CM.

d. Basic Attributes of Data Managed by an ECM Program. The following four attributes help determine whether a given data item is properly managed under ECM procedures. For an ECM program to be fully effective, all four of these attributes must apply. Data must be—

(1) **Authoritative.** Data must show the latest, approved version.

(2) **Attributable.** Data must show who created or modified the latest version.

(3) **Searchable.** Data must be created and stored in a way that enables others to find it.

(4) **Archiveable.** Previous data versions must be preserved.

6. RECORD RETENTION REQUIREMENTS

a. Organizational CMs must train their organization's personnel on data-retention requirements for documents that personnel use and create. Specifically, personnel must understand the difference between "T" and "K" records (AR 25-400-2).

(1) "T" Records must be kept, transferred, and disposed of according to specific record retention schedules.

(2) "K" Records will be kept no longer than 6 years, unless their value beyond that date can be justified.

b. The retention requirement for a file with a date showing that it was created or last modified more than 6 years ago must be coordinated with the listed owner (or his or her replacement) to determine the validity of the file and why it should be retained. The owner is responsible for removing documents that have expired or are no longer needed.

7. NAMING CONVENTIONS AND VERSION CONTROL

Naming conventions comprise a set of rules for naming documents. The name of a document should readily describe the document's content. Naming conventions reduce the amount of time and effort needed to determine what data is in a document and the date it was created or last used. All Army in Europe personnel will use the following naming conventions when creating documents.

a. Naming Documents. Documents that will be saved as files must be named in the following format: *date-originator-object-version number-disposition*. The date must be in the YYYYMMDD format, and the version number will include a lowercase *v* and a two-digit number (for example, *v01* is version 1). If named correctly, the file will be self-defining. The following are examples of descriptive document names following the prescribed format:

(1) 20110501-G3-Monthly-Status-Report-v01-draft.doc.

(2) 20110601-G6-Annual-Performance-Report-final.doc.

NOTE: Document file names should be limited to no more than 50 characters to ensure that all systems, such as SharePoint, will accept and recognize the file. (For example, files with names that are longer than 50 characters cannot be uploaded in SharePoint.)

b. Best Business Practices. The following BBPs must be applied when naming files:

- (1) Use a file name that describes the contents.
- (2) Use hyphens instead of periods or spaces.
- (3) Format dates consistently using the YYYYMMDD format.
- (4) Include the version number of the document even if only one version exists.
- (5) Avoid using special characters.
- (6) Ensure that file names are consistent.

c. Naming Folders. Folder names must be short to allow for descriptive file names without exceeding the 255 file-path character limit. Folders should be named for a department, topic, or category. Position titles rather than personal names may also be used for folders created by or for an individual in the organization. Using position titles instead of personal names helps prevent folders from being deleted when an individual leaves the organization. Existing folders should be periodically reviewed to identify duplicate or significantly overlapping folders.

d. Version Control. Version control involves the management of changes made to documents. Local hard drives and an organizational shared drive do not provide version control. Consequently, naming conventions are the only way to ensure authoritative versions of documents are used. To ensure version control—

(1) Draft versions of documents will include the word “draft” and indicate the file version in the document name (for example, 20110501-G3-Alert-Roster-v01-draft.doc).

(2) Final documents will include the word “final” as part of the document name (for example, 20110501-G3-Alert-Roster-final.doc).

(3) Once a document has been finalized, any draft and comment versions should be deleted.

(4) When working in SharePoint, the version-control application should always be enabled.

8. PORTAL BRANDING REQUIREMENTS

For ease of use and to ensure consistency throughout the Army in Europe, all portals must be designed according to the branding requirements prescribed by this regulation. Table 1 lists the requirements.

Portal Object	Page Location	Description
Theme		Will be "Army."
Global Breadcrumbs	Top left	A link, typically at the top left of the page, taking the user back to the homepage.
Welcome Menu	Upper right	Places a welcome message and allows users to log out.
My Sites	Upper right	A link to the My Sites functionality, which allows end users to have their own personalized portal with their favorite content. My Sites usually is appropriate only on intranet sites.
My Links	Upper right	Similar to My Sites, but allows end users to collect links that are important to them. My Links is appropriate only on intranet sites.
Help Icon	Upper right	An icon that links to SharePoint help. The Help icon is usually not appropriate on Internet-facing sites.
Site Actions	Upper right	This menu will be used by all administrators and content authors. It is the main menu for interacting with a Microsoft Office SharePoint Server (MOSS) site.
Site Title	Top left above Global Breadcrumbs	A brief line of text that tells the user the title of the current site.
Search Box	Top right	In publishing sites, either of two types of search boxes that can be used: one with search scopes or one with the advance search link.
Top Navigation	Top right	A fairly critical part of any MOSS site, this is the main means of site navigation.
Page Breadcrumbs	Top left	A breadcrumb trail that shows how the user navigated to the current page.
Left Navigation	Left, top to bottom	A helpful way of navigating the MOSS site. Sometimes this is used as secondary navigation.
Main Content	Center	This is the actual content of the page. Portal designers may choose where to place it in the layout.
Organization Chart	Clearly posted link on the left navigation column	A hierarchical chart that shows as a minimum the roles and contact information of an organization's division chiefs.
Site Content Manager Contact Information	Bottom right	All pages will have the organization's enterprise CM listed with e-mail and telephone contact information. All pages will have a "date of last modification" entry included with the enterprise CM contact information.

9. METADATA

Each organization will appoint a metadata manager who will be responsible for developing and implementing a metadata strategy. Applying a metadata strategy will ensure that metadata is always complete, current, and correct. This strategy will also ensure that users understand how to use metadata. The metadata manager and CMs must continually monitor metadata to ensure that organizational data corresponds with organizational requirements. Users who upload content to the EUR SharePoint Portal, a shared drive, or a website must ensure that the metadata is accurate and complete. The metadata manager and CMs, or their designated alternates, will ensure that metadata for content uploaded to publicly accessible websites is accurate. More details regarding metadata policy are available at <https://portal.eur.army.mil/sites/kmo/projects/md/default.aspx>.

a. Key Types of Metadata and Descriptions.

(1) Descriptive Metadata. Descriptive metadata is data used to search and locate an object such as a title, an author, subjects, keywords, or a publisher.

(2) Structured Metadata. Structured metadata describes how the components of an object are organized.

(3) Administrative Metadata. Administrative metadata refers to technical information including the file type. Two subtypes of administrative metadata are rights-management metadata and preservation metadata.

(4) Technical Metadata. Technical metadata defines objects and processes in a data warehousing/business intelligence (DW/BI) system. Technical metadata includes the system metadata, which defines data structures such as tables, fields, data types, indexes and partitions in the relational engine, databases, dimensions, measures, and data-mining models. Technical metadata also defines the data model and the way it is displayed for the users, with reports, schedules, distribution lists, and user security rights.

(5) Business Metadata. Business metadata summarizes content from a data warehouse in more user-friendly terms using word “tags.” These tags show users the type of data they have, where it comes from, what it means, and what its relationship is to other data in the document warehouse. Business metadata may also serve as documentation for the DW/BI system. Users who browse the data warehouse are primarily viewing metadata.

(6) Process Metadata. Process metadata is used to describe the results of various operations in the data warehouse. Within the extract, transform, and load (ETL) process, all key data relating to tasks is logged when tasks are carried out. This includes start time, end time, seconds used by the central processing unit, disk reads, disk writes, and rows processed. This type of data is useful when troubleshooting the ETL or query process. Process metadata provides the measurements for building and using a DW/BI system. Process metadata can be used to see which users are using various products, and to see what level of service those users are receiving.

b. Metadata Management. Metadata management involves storing information about other information. With different types of media being used, references to the location of data allow for the management of diverse repositories.

10. DATA RETENTION AND ARCHIVING

There are several methods of storing information, all of which must be regularly reviewed to ensure only proper content is retained. Each of the storage alternatives has its own strengths and weaknesses and presents different challenges to ECM.

a. USAREUR SharePoint Portal. The SharePoint portal is the primary collaboration tool used by the HQ USAREUR staff and the staffs of USAREUR MSCs. It should be used when files need to be accessible by members of other organizations within the EUR domain. Although the portal is accessible to visitors from outside the EUR domain, permissions can be easily set to restrict access to those who need to see specific information on the portal. The portal allows several users to contribute to the development of a document and provides versioning and access-control capabilities. Portal data is routinely backed up.

b. Local Computer. Users may store documents on their local computers (usually under “My Documents”), provided no one else needs access to the documents. Users tend to use this option when working on drafts; but when doing so, users must keep in mind that their drafts will not be accessible to anyone else. Users also need to remember that data stored on local computers is not backed up. Users typically do not manage the content of their documents on a local computer according to the conventions established in paragraph 7a; but once the user is ready to move the document to a shared folder for general use, or once the disk on the local computer is full and the data needs to be moved and stored elsewhere, the principles of ECM, such as naming conventions, must be applied.

c. Shared Drives. USAREUR provides additional storage space to anyone on the network, subject to the permissions established by the creators of shared folders. Generally speaking, organizations in the Army in Europe (specifically those on the EUR domain) have the ability to establish shared folders on a central data server. Those organizations can then create and give specific permissions to members of the EUR domain so they may have access to the data in the shared folders. By saving a document in a shared folder or in a shared subfolder and informing others of the location of the document, information can be easily shared. Another advantage of shared folders is that shared drives are regularly backed up. The main problem with shared drives and folders is that they fill up quickly as a result of many contributors working on collaborative projects. Applying the principles of ECM is therefore essential when storing documents on shared drives.

d. USAREUR Homepage. The USAREUR homepage (<http://www.eur.army.mil/>) is USAREUR’s primary medium for sharing information with an external audience. The homepage is not designed, however, to be used for routine storage of internal USAREUR data. The Office of the Chief, Public Affairs (OCPA), HQ USAREUR, monitors the homepage to ensure information is released in a planned and controlled manner to avoid violations of operations security. The OCPA also monitors use of the site by anyone granted access as a contributor.

e. Army Knowledge Online (AKO). AKO is a portal similar to the USAREUR SharePoint portal, offering most of the same features and capabilities. It supports the modification and storage of documents and version-control capabilities. Anyone can gain access to the AKO portal through an AKO account, through a password or common access card (CAC) authentication. Consequently, information stored on the AKO portal is less secure than the information on the USAREUR portal. Therefore, the AKO portal should be used for storage only when no other method of sharing information will meet the particular requirement.

f. Offline Storage on Digital Versatile Disk (DVD) or Compact Disk (CD). Once a document no longer needs to be readily available, it should be stored offline. Local information management offices provide instructions on how to store data on DVDs and CDs. DVDs and CDs must be properly labeled (for example, marked UNCLAS) and secured. Information that is For Official Use Only (FOUO) must be kept in either a locked office or locked container. Classified information must be protected in approved security containers or open storage areas. Unit security managers can provide details on proper storage procedures.

g. Hardcopy Storage. Printed information must be maintained in accordance with AR 25-400-2. In some cases, FOUO or classified documents must be available in a hardcopy format (for example, continuity of operation and disaster recovery plans). Such information must be protected in the same way as the DVDs and CDs that hold FOUO or classified information (f above). The USAREUR Records Administrator at DSN 370-8804 can provide more information on hardcopy storage procedures.



DEPARTMENT OF THE ARMY
UNITED STATES ARMY EUROPE
Unit 29351
APO AE 09014-9351

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE KNOWLEDGE MANAGEMENT BRANCH, OFFICE OF THE DEPUTY CHIEF OF STAFF, G3,
HQ USAREUR
AND
HQ USAREUR STAFF AND ORGANIZATIONAL CONTENT MANAGERS

SUBJECT: Roles and Responsibilities of the Knowledge Management Branch, Office of the Deputy Chief of Staff, G3, HQ USAREUR, and HQ USAREUR Staff and Organizational Content Managers

- 1. Purpose.** This memorandum identifies the roles and responsibilities of the Knowledge Management (KM) Branch, Office of the Deputy Chief of Staff, G3, HQ USAREUR, and HQ USAREUR staff and organizational content managers (CMs).
- 2. Problem.** Enterprise content management (ECM) has been an issue within the USAREUR NIPRNET and SIPRNET portals. Users have experienced difficulties in locating documents after uploading them to SharePoint and during the collaboration process.
- 3. Solution.** Instituting the use of ECM through well-trained CMs will help ensure that files can be managed, tracked, and found.
- 4. Scope.** This memorandum applies to the staff of the KM Branch, HQ USAREUR, and organizational CMs.
- 5. Responsibilities.**
 - a. CMs will—
 - (1) Ensure staffs are trained in all aspects of ECM.
 - (2) Conduct monthly assessments and maintenance of all document libraries within their sites to ensure documents meet all ECM requirements.
 - b. The staff of the KM Branch will—
 - (1) Ensure that CMs understand ECM policy and procedures.
 - (2) Perform quarterly portal assessments to ensure compliance with USAREUR ECM policy.
- 6. Effective date.** This memorandum becomes effective on the date signed by all parties.

Content Manager
Signature Block

Date

ANDREW S. FLETCHER Date
LTC, AR
Chief, KM

Figure 1. Memorandum of Understanding Between the Knowledge Management Branch, Office of the Deputy Chief of Staff, G3, HQ USAREUR, and HQ USAREUR Staff and Organizational Content Managers



DEPARTMENT OF THE ARMY

Organization Name
Unit XXXXX
APO AE XXXXX-XXXX

Office Symbol

Date

MEMORANDUM FOR USAREUR G6 (AEAIM-O)

SUBJECT: Appointment of SharePoint Site Collection Administrator for *Organization Name*

1. The following individual or Active Directory group is appointed as the primary SharePoint site collection administrator for URL <https://portal.eur.army.mil/sites/XXX>.

Account: _____ (for example, EUR\joe.doe)

2. Authority.

a. AR 25-1, Army Knowledge Management and Information Technology
(http://www.army.mil/usapa/epubs/25_Series_Collection_1.html).

b. AE Regulation 25-71, Website Administration
(<https://aepubs.army.mil/ae/public/publications-list.aspx?Pub=AE%20REG>).

c. DOD Web Site Administration Policies & Procedures
(http://www.defenselink.mil/webmasters/policy/dod_web_policy_12071998_with_amendments_and_corrections.html).

3. This memorandum supersedes all previous memorandums of the same subject.

Commanding Officer
Signature Block

CF:
USAREUR G6 (AEAIM-O/Software Engineering Branch)

Figure 2. Sample Appointment Memorandum for a SharePoint Site Collection Administrator

GLOSSARY

AE	Army in Europe
AKO	Army Knowledge Online
AR	Army regulation
ARIMS	Army Records Information Management System
BBP	best business practice
CD	compact disk
CM	content manager
DA	Department of the Army
DOD	Department of Defense
DVD	digital versatile disk
DW/BI	data warehousing/business intelligence
ECM	enterprise content management
ETL	extract, transform, and load
FOUO	For Official Use Only
KM	knowledge management
MOSS	Microsoft Office SharePoint Server
MSC	major subordinate command
OCPA	Office of the Chief, Public Affairs, HQ USAREUR
USAREUR	United States Army Europe
USAREUR G3	Deputy Chief of Staff, G3, United States Army Europe