

**BY ORDER OF THE COMMANDER
WRIGHT-PATTERSON AIR FORCE
BASE**

**WRIGHT-PATTERSON AIR FORCE
BASE INSTRUCTION 33-301
12 MAY 2016**



Certified Current 28 June 2018

Communications and Information

***ENTERPRISE INFORMATION
SERVICES (EIS) AND THE AIR FORCE
(AF) PORTAL***

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication

OPR: 88 CS/SCOKW

Certified by: 88 CS/CC
(Lt Col Brian L. Snyder)

Supersedes: WRIGHTPATTERSONAFBI
33-301, 4 April 2013

Pages: 20

This publication implements policy and best practices published in the site collection repository of HQ AFMC/A6 and AFI 33-115, *Air Force Information Technology (IT) Service Management*, and is intended for all site owners, content managers and users of information located in the document libraries of EIS and content of the AF Portal. This publication applies to the 88th ABW and supported tenant organizations at Wright-Patterson AFB. This publication does not apply to AFRC and ANG units. Send comments and suggestions about this publication for improvements on AF Form 847, *Recommendation for Change of Publication*, to the Office of Primary Responsibility (OPR). Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363, Management of Records, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

SUMMARY OF CHANGES

Minor changes have been made to update URLs, update training sources, and update a reference from AFI 33-129 to AFI 33-115.

1. Introduction:

1.1. AFMC Enterprise Information Services (AFMC EIS) is a web enabled, information technology based platform providing a set of capabilities supporting many knowledge worker tasks. The goal of AFMC EIS is to improve awareness, knowledge, accuracy and

productivity of AFMC workers through the deployment of standard enterprise Information Technology (IT) resources that facilitate standard information management and knowledge operations processes. EIS consists of Active Risk Manager (ARM), Project Server, Enterprise Information Management (EIM), and other capabilities.

1.2. The Air Force (AF) Portal provides Enterprise/Centralized content for all AF Organizations, Bases, Functional Areas and Organizations outside AF, DoD and non-DoD partners and Allied Forces. The goal of the AF Portal is to provide information to the rest of the Air Force as it pertains to your Organization and is accessible to all military and civilian personnel, as well as approved users, 24/7 via .mil/.com.

2. Background:

2.1. In 2007, SAF/A6 & CIO and SAF/AA approved Microsoft SharePoint as the document management and workflow capability tool to enhance the AF Enterprise Information Management (EIM) project--an initiative to deploy a set of standard office automation solutions. AFMC EIS guidance is provided in memorandums signed by SAF/XC and AFMC/CC ([Attachment 2](#) and [Attachment 3](#)).

2.2. Since 2008, the AF Portal has been the designated source for hosting all AF enterprise level static web content; while eliminating the use of private .mil websites and servers. In this document, users will gain a better understanding of what their role and responsibilities are, to include proper permission assignment, content management review and required documented training records.

3. Roles and Responsibilities: The following instruction provides guidance condensing information from the EIS/EIM Support Center, but is not all inclusive and not limited to:

3.1. EIM.

3.1.1. Unit Commanders will:

3.1.1.1. Identify a primary and alternate Site Owner for Organizational and Community sites and ensure new appointees visit the EIM Support Center to familiarize themselves with SharePoint and take the self-paced training and/or attend the Site Owners training course offered by the Education & Training Flight.

3.1.1.2. Provide appointment letter and proof of EIM training signed by the Unit Commander to wing or base content manager. See [Attachment 6](#), appointment letter. This letter and proof of EIM training can also be copied and pasted into an email and electronically signed by the Unit Commander.

3.1.2. Site Owners/Users:

3.1.2.1. Are responsible for understanding and following the AFMC EIM concepts contained in this instruction and on the EIS/EIM Support Center.

3.1.2.2. EIM should be used as a collaboration tool for doing day-to-day work. It is not a replacement tool for the Electronic Records Management (ERM) system and not approved as an official records management repository.

3.1.2.3. Will review document libraries housing folders/documents every 180 days in an effort to move Air Force records to the ERM, and eliminate duplicated documents,

archived information and improperly marked restricted areas. Reference EIM Site Owner Review Procedures para 3.1.10.

3.1.2.4. Will ensure appropriate permission assignment is given to document libraries containing folders/documents with Privacy Act (PA)/Personally Identifiable Information (PII), Source Selection Sensitive, Scientific and Technical Information (STINFO), Foreign Disclosure, Export Control Laws and any data driven by law or regulation. Reference business practices para 3.1.8.3. and para 3.1.8.4.

3.1.2.5. Site owners/users are prohibited from purchasing or installing SharePoint outside of the AFMC EIM. **NOTE:** commercial software, government off-the-shelf technology and local development are specifically prohibited). EIM is the official Air Force collaboration tool. EIM is to be used as a unit/organization's area for hosting dynamic content and active files for conducting day-to-day operations and business. Use of shared drives should be minimized and shared drives should not be used instead of EIM. Official records will not be permanently stored in EIM, but rather be moved to ERM when made a final draft for record.

3.1.3. Business Practices.

3.1.3.1. Information is shared to the widest extent possible. Visitor permissions will be enabled in EIM as read-only by default. There is a tendency to lock down permissions on EIM folders unnecessarily by default. The exception is Controlled Unclassified Information (CUI) which is restricted from dissemination by laws, regulations, and policies. Some of these classifications are Privacy Act Information, Source Selection Sensitive, Intellectual Property (e.g. company proprietary and trade secrets), Information subject to the foreign disclosure and/or export control laws, Scientific and Technical Information (STINFO) (e.g. weapon system technical publications) and Foreign Disclosure. The culture of the knowledge worker should be one of information sharing instead of information hoarding. DoDI 8320.02 para 3.a. states: "Data, information, and IT services are considered enablers of information sharing to the DoD. Data, information, and IT services will be made visible, accessible, understandable, trusted, and interoperable throughout their lifecycles for all authorized users. Authorized users include DoD consumers and mission partners, subject to law, policy, data rights, and security classifications."

3.1.3.2. Everyone is a visitor. Every organization site or community site front page, no matter how "buried" it is in the site collection, will be open to all authenticated AFMC personnel with "visitor" permissions (by selecting "NT AUTHORITY\authenticated users"). This will maximize collaboration, let people know the community or an organization exists, and let people see who the leadership or POCs are to find out more about that organization or community. Exceptions to this rule are top level source selection team sites, subsites dedicated to an organization's personnel activities, or other sites/subsites dedicated to information that has a legal obligation to secure, i.e., CUI as described in para 3.1.8.1.

3.1.3.3. FOUO Information Protection. For Official Use Only (FOUO) information is unclassified information that may be exempt from release under the Freedom of Information Act (FOIA) under exemptions 2 through 9 of the FOIA, and the Privacy Act (PA) of 1974. FOUO generally needs no special protection under EIM as EIM is

inclusive to DoD. FOUO is not authorized as an anemic form of classification to protect national security interests. (DoD Reg 5400.7/AF Sup, DoD FOIA Program, C4.1.1). Exemptions from disclosure to the public will be coordinated through the Base FOIA/PA Manager to ensure legal ramifications are considered. Subject matter experts can contact the FOIA/PA Office at 937-522-3095 for further information.

3.1.3.4. Mark all information requiring restricted permissions. Documents uploaded to restricted areas will be marked appropriately for the types of data they contain (such as “FOUO”, “Privacy Act” or “STINFO”).

3.1.3.5. Minimize full control permissions. Site owners with full control permissions should be kept to a minimum (two to three personnel) for site integrity and security.

3.1.3.6. Assign permissions to groups, not individuals. Assigning individual permissions creates a permissions environment that is difficult to manage. Site-wide permissions for groups can be viewed, individual permissions cannot. Group permissions support a role based permissions environment which allows a departing individual to be replaced by a new individual easily – the new individual inherits all of the correct permissions for the role.

3.1.3.7. AFMC Templates. When setting up a new page or subsite, site owners will use the AFMC templates. (e.g. AFMC document library, AFMC standard organization, and the AFMC community site templates).

3.1.3.8. Document library restricted permissions. Libraries will have an (R) appended to the end of the document library name to notate a document library with restricted permissions. The description will contain notice as to why it is restricted and to what groups it is restricted for future reference.

3.1.3.9. Unique Permissions. Do not create unique permissions for items below the container (subsite/list/library) level unless absolutely necessary (e.g. alert rosters, timecards, finance/GPC, other CUI/PII-driven processes).

3.1.3.10. Versioning. Always use the AFMC Document Library template which will enable versioning for all libraries for five previous versions.

3.1.3.11. Group Names. Group names should always begin with the site name.

3.1.3.12. Container Descriptions. Always include a detailed description of the container. Any time you create a site, library, or list, BE SURE to provide a DESCRIPTION of the container. Include the purpose, type of information allowed, intended audience, and whether the container is restricted access. (For libraries, also include in the description the number of versions enabled if changed from the default).

3.1.3.13. EIM training. Site members and site owners will use standardized AFMC-provided EIM training. Standardized training may be supplemented but cannot contradict AFMC EIM training guidance. Two sources of classroom training are classes offered during 88 ABW Focus Week and training provided by the Education & Training Flight (88 FSS/FSDE).

3.1.3.14. Tactics, Techniques, and Procedures (TTP). Personnel will reference and follow approved EIM Tactics, Techniques, and Procedures on the TTP page at <https://cs.eis.afmc.af.mil/sites/eisusersupport/eimsupportcenter/pages/TTPs.aspx>

3.1.4. Document Management.

3.1.4.1. One working copy in one location. Links will point to one working copy in lieu of uploading multiple copies of a document. The document should be checked out for editing and checked back in when editing is completed. This will prevent changes from being overwritten by preventing the document from being edited by more than one person at a time.

3.1.4.2. Send URLs instead of attachments in e-mail. Personnel will send EIM, ARM, Project Server, Air Force Portal, or internet uniform resource locator (URL) document links via E-mail and not the actual documents. This applies only within an enclave that is accessible by all. Document attachments may still be sent via E-mail when necessary (i.e. leaving AFMC). A URL can be inserted as a hyperlink with a convenient name. Follow Tip 15 (Inserting EIM links into E-mail) at: <https://cs.eis.afmc.af.mil/sites/eisusersupport/eimsupportcenter/TipOfTheWeek/Forms/Input%20View.aspx>.

3.1.4.3. Maximum four folders deep. The number of nested folders (folders within folders) in a document library will be kept to four levels (a folder within a folder within a folder within a folder within a document library at the maximum). Zero folders up to two nested folders is ideal. Too many nested folders in a document library leads to buried information and difficult navigation for the user. An additional technical limitation driving limiting nested folders is that EIM only works with URLs up to 260 characters long. In lieu of multiple folders, files can be grouped by using file name conventions within a folder. (TTP RM-02) <https://cs.eis.afmc.af.mil/sites/eisusersupport/eimsupportcenter/pages/TTPs.aspx>

3.1.5. **EIM Site Owner Review Procedures.** For AFMC EIM to provide a secure and consistent experience for the community, it is essential that a periodic review of all AFMC EIM Organization, Community, Conference Room, and 'Team' sites be conducted at least every 180 days. This review will ensure that EIM sites are up-to-date, consistent, and have proper permission structures in place.

3.1.5.1. Check Site Content. Is the site content consistent with the type of site? Organization site content is to be used for the "care and feeding" of the personnel in the organization. Community site content is to be used to support the "work or services" the organization does, and to allow collaboration between the organization and its customers.

3.1.5.2. Check Site Permissions. Select "Site Actions" then "Site Settings" then "Advanced Permissions." Does the site use "unique permissions" with its own set of Member, Owner, and Visitor site groups? (The rare exception withstanding, an organization or community site should not inherit permissions from its parent. If the permissions from the parent site support the child site, why was the child site required? A reworking of the Site's permissions may be required).

3.1.5.3. Check Site Groups for permissions. Are permissions provided only to Site Groups? The AFMC EIM design only allows the assignment of permissions to “EIM Groups.” Direct assignment to Active Directory (AD) groups, Exchange groups or Individuals will be difficult to maintain. Use a lot of forethought when deciding how many Site Groups to use. Even Site Groups need maintenance now and then. If updates or additional groups are needed, use the following steps.

3.1.5.3.1. Create new Site Groups to support the roles related to the site.

3.1.5.3.2. Move individual users or AD/Exchange groups into the appropriate Site Group based on the related role.

3.1.5.3.3. It may be necessary to create new AD groups to support functional roles that require access across multiple Site Collections.

3.1.5.4. Does each Site Group have only one “Permission Level?” Only one “Permission Level” (Contribute, Full Control, Read) should be assigned to a given site group. The “Permission Levels” typically include all of the lower level permission settings. Restricted/Modified Permissions. It is possible and permitted, to break permission inheritance on Lists, Libraries, and Folders when absolutely required.

3.1.5.5. Check Access Requests. Select “Settings” then “Access Requests.” Is “Allow requests for access” checked and a Site Owner email provided?

3.1.5.6. Check People and Groups. Select “Site Actions” then “Site Settings” then “People and Groups.” Do the local Members, Owners, and Visitors (MOV) groups display in the “Group Quick Launch” (Quick Launch Bar on left side of EIM site)? If not edit the “Group Quick Launch” accordingly.

3.1.5.6.1. For each local MOV group select “Setting” then “Group Settings.”

3.1.5.6.1.1. The title should start with the site name.

3.1.5.6.1.2. The group owner should be the Site Owners group.

3.1.5.6.1.3. The membership should be visible to “Everyone.”

3.1.5.6.1.4. The editor of the group should be the Site Owners group.

3.1.5.6.2. Check the membership of the Members group. Is the membership of the Members group consistent with the data on the “Site Information Form?” For organization sites this typically means the “Org All” Active Directory group has been added, and for Community sites individuals or Functional Active Directory Groups have been added.

3.1.5.6.3. Check the membership of the Owners group. Is the membership of the Owners group consistent with the data on the “Site Information Form?” AFMC EIM is looking for 2-3 Site Owners for a given site.

3.1.5.6.4. Check the membership of the Visitors group. Is the membership of the Visitors group consistent with the data on the “Site Information Form?” Usually this means it is the system entry “NT AUTHORITY\authenticated users” to open the site to all of AFMC.

3.1.5.7. Check the Nested Folders in a Document Library. Is the number of nested folders (folders within folders) kept to a maximum of four? Too many nested folders in a document library leads to buried information and difficult navigation for the user. Zero folders up to two nested folders is ideal.

3.1.5.8. Check Site Theme. Select “Site Actions” then “Site Settings” then “Site Theme.” Is the site theme set to the AFMC EIM Standard based on site type? Are the standard web parts in place? Leadership, site assistance, logo? Is extra content added below standard content?

3.1.5.8.1. “Lichen” for Organization sites.

3.1.5.8.2. “Belltown” for Community sites.

3.1.5.8.3. “Breeze” for Conference Room sites.

3.1.5.8.4. “Classic” for Team sites.

3.2. AF Portal:

3.2.1. Unit Commanders will:

3.2.1.1. Ensure their AF Portal Content Managers and Content Publishers receive training on portal publishing (**AF Portal Publishing Training (AFPPT)**) and ensure this training is documented.

3.2.1.2. Appoint their AF Portal Content Managers and Content Publishers in writing. Unit Content Managers and Content Publishers should be a knowledge operations manager (AFSC3A0XX or civilian equivalent) to the maximum extent possible. The wing or base level Content Manager will maintain the appointment letters for their organization.

3.2.1.2.1. Provide appointment letter and proof of Portal training signed by the Unit Commander to wing or base content manager. See **Attachment 4**, appointment letter. This letter and proof of Portal training can also be copied and pasted into an email and electronically signed by the Unit Commander.

3.2.2. **Wing/Group/Unit AF Portal Content Manager.** Each group/unit supplying AF Portal page information for posting on the AF Portal appoints an AF Portal Content Manager responsible for information on their respective pages. Group/Unit Content Managers will:

3.2.2.1. Ensure a process is in place for posting information to their respective AF Portal page(s).

3.2.2.2. Approve content posted to the AF Portal.

3.2.2.2.1. Ensure proper review of any content containing PA, FOUO, PII, FOIA, Contracting, Financial, Legal and Foreign Disclosure information.

3.2.2.2.1.1. Document the review using the Portal IRP, see **Attachment 5**. Provide a copy to the wing or base level AF Content Manager. Group/Unit Portal Content Manager will maintain the original.

3.2.2.2.1.2. Establish security and role restriction requirements before posting

information on the AF Portal.

3.2.2.2.2. All Portal pages must be reviewed at least every 180 days. Update the last reviewed date under the Contact the Content Manager area of the Portal page after the review is completed.

3.2.2.2.2.1. Validate all links on AF Portal pages within their span of control on a quarterly basis. 3.2.2.2.2.2. On top level page:

3.2.2.2.2.2.1. Content Manager's organization, office symbol, commercial phone number, and DSN.

3.2.2.2.2.2.2. Organizational email addresses. Date last reviewed (pages/links must be reviewed at least every 180 days).

3.2.2.2.3. Identify and update or remove incorrect or superseded information.

3.2.2.3. Oversee unit AF Portal page development and maintenance. Ensure compliance with all laws and policies such as in 29 U.S.C. § 794d, Rehabilitation Act of 1998, Section 508, as amended by Public Law (PL) 105-220, Workforce Investment Act of 1998.

3.2.2.3.1. Approve personnel for Content Publisher access and provide training on policy, processes and guidelines for posting information to the AF Portal.

3.2.2.3.2. Request organizational structure changes and modify existing structure according to publishing guidelines available on the AF Portal publishing training page.

3.2.2.3.3. Complete minor structural changes. These changes may be accomplished through tiered publishing permissions and a work flow process.

3.2.2.3.4. Maintain delegation letters/spreadsheet and proof of training for Content Managers under their purview. Follow appropriate disposition guidance related to delegation letters.

3.2.2.3.5. Work with the Content Publisher to remove or correct instances of sensitive or inappropriate information on AF Portal pages in accordance with PA procedures.

3.2.3. Content Providers will:

3.2.3.1. Ensure proper review and approval of material by the appropriate offices.

3.2.3.2. Account for the classification, currency, sensitivity, and release of the information.

3.2.3.3. Validate the accuracy of all material provided to the AF Portal Content Publisher.

3.2.3.4. Comply with PA requirements (i.e., safeguard personal information, post PA statement and Privacy Advisories) see AFI 33-332, when collecting PA information from individuals).

3.2.3.5. Be accountable in the event of unauthorized disclosure of information on the AF Portal.

3.2.4. **PII.** Names and e-mail addresses may be posted to private Web sites (restricted to .mil or .gov users) at the discretion of the local commander, when necessary to conduct official business, and after conducting the appropriate risk assessment. The risk assessment should balance the operational benefit of posting the personal information against the risk of unauthorized disclosure or alteration. The following areas should be considered in your assessment: official purpose for posting the information; possible vulnerabilities and threats to the information; the potential impact of unauthorized disclosure or modification of the information; the security of your network and existing safeguards (hardware, software, local administrative Web guidance/policy).

RICK T. JOHNS, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

29 U.S.C. & 794d, Rehabilitation Act of 1998, Section 508, as amended by Public Law (PL) 105-220, Workforce Investment Act of 1998, <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards>.

AFI 33-115, *Air Force Information Technology (IT) Service Management*, 16 September 2014

AFI 33-332, *Air Force Privacy and Civil Liberties Program*, 12 January 2015

AFMAN33-363, *Management of Records*, 1 March 2008

AF Portal Content Management training URL, <https://www.my.af.mil/gcss-af/USAF/ep/globalTab.do?channelPageId=sA4057E1F290AE3E80129367B34060462>.

AF Portal Content Manager Training Guide, https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC133F560FB5E044080020E329A9/Files/editorial/AF_Portal_Content_Manager_Training_Guide_V4.1.pdf?channelPageId=s6925EC133F560FB5E044080020E329A9&programId=tA1FBF31D21207A07012132BC06AB0268.

AF Portal Content Publisher Training Guide, https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC133F560FB5E044080020E329A9/Files/editorial/AF_Portal_Content_Publisher_Training_Guide_V3_20100615.pdf?channelPageId=s6925EC133F560FB5E044080020E329A9&programId=tA1FBF31D21207A07012132BC06AB0268.

AF Portal Overview Training Guide, https://www.my.af.mil/gcss-af/USAF/AFP40/d/s6925EC133F560FB5E044080020E329A9/Files/editorial/AF_Portal_Overview_Training_Guide_V3_20100615.pdf?channelPageId=s6925EC133F560FB5E044080020E329A9&programId=tA1FBF31D21207A07012132BC06AB0268.

AF Portal Publishing Training (AFPPT), <https://www.my.af.mil/gcss-af/USAF/ep/globalTab.do?channelPageId=s6925EC133F560FB5E044080020E329A9>.

AFMC EIM Tactics, Techniques, and Procedures (TTPs), <https://cs.eis.afmc.af.mil/sites/eisusersupport/eimsupportcenter/pages/TTPs.aspx>.

EIM Support

Center, <https://cs.eis.afmc.af.mil/sites/eisusersupport/eimsupportcenter/default.aspx>.

Adopted Form

AF Form 847, *Recommendation for Change of Publication*

Terms

AFMC—Air Force Materiel Command

EIM—Enterprise Information Management

EIS—Enterprise Information Services

FOIA—Freedom of Information Act

FOUO—For Official Use Only

IRP—Internet Release Package

PA—Privacy Act

PII—Personally Identifiable Information

STINFO— Scientific and Technical Information

Attachment 2

WEB CONTENT MIGRATION GUIDANCE MEMORANDUM

Figure A2.1. Web Content Migration Guidance Memorandum.



DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC

OFFICE OF THE SECRETARY

21 Nov 2008

MEMORANDUM FOR MAJCOM CVs AND FUNCTIONAL 2-LETTERS

FROM: SAF/XC
1800 Air Force Pentagon
Washington, DC 20330-1800

SUBJECT: Web Content Migration Guidance

References: (a) SAF/XC, Web Content Migration Memorandum, 13 Jun 2006
(b) SECAF/CSAF, IT Initiatives Policy Memorandum, 3 Dec 2003
(c) AF-CIO/S, Web Content Migration Plan Memorandum, 2 Jul 2004

To date, the Air Force has migrated 91 percent of our static web content to the Air Force Portal and have eliminated most private .mil websites and servers. However, we must continue the migration of static web content in order to realize resource savings and improve security. This memorandum provides supplemental migration guidance to the IT Initiatives Policy Memorandum dated 3 Dec 2003. Moreover, this memorandum supersedes the Web Content Migration Plan and Migration Memorandums dated 2 Jul 2004 and 13 Jun 2006, respectively.

All Air Force organizations will migrate their remaining private and internal static web content to the Air Force Portal, Air Force Knowledge Now, or AFNet/MAJCOM Enterprise Information Management (EIM) Microsoft Office SharePoint Server (MOSS) environments, as prescribed below:

- The Air Force Portal will be the authoritative source for hosting Air Force enterprise-level static web content.
- Air Force Knowledge Now will host static and dynamic web content that supports person-to-person or working-group collaboration and information.
- AFNet/MAJCOM EIM MOSS environments may host static and dynamic web content internal to that organization.

Attachment 1 provides suggested content placement examples and attachment 2 contains guidance for reporting migration progress/metrics. Our points of contact for web content migration are Col Robert Kaufman, SAF/XCDI, DSN 425-1511, Mr. Gino Faulkner, SAF/XCDI, DSN 425-7804, and Capt Eric Simmons, AFCA/ECSS, DSN 779-6462.

A handwritten signature in black ink, appearing to read "Michael W. Peterson".

MICHAEL W. PETERSON, Lt Gen, USAF
Chief of Warfighting Integration and
Chief Information Officer

Attachment 3

AFMC EIS GUIDANCE MEMORANDUM

Figure A3.1. AFMC EIS Guidance Memorandum.



DEPARTMENT OF THE AIR FORCE
 HEADQUARTERS AIR FORCE MATERIEL COMMAND
 WRIGHT-PATTERSON AIR FORCE BASE OHIO

MEMORANDUM FOR ALHQCTR/CC/CL
 ALHQSTAFF
 ALINST/CC/CL

30 MAR 2010

FROM: AFMC/CC
 4375 Chidlaw Road
 Wright-Patterson AFB OH 45433-5001

References: (a) SAF/XC Memo, 21 Nov 08, Web Content Migration Guidance (Atch 1)
 (b) AF ERM Guide, 4 Sep 07, Electronic Records Management (ERM)
 Solution (Atch 2)

SUBJECT: AFMC Enterprise Information Services (EIS) Guidance Memorandum

1. HQ AFMC/A6/7 and the AFMC communications/chief information officer community have fielded a standardized set of EIS capabilities which include document management, business process automation, collaboration, and enterprise-wide information search as a core communications service. EIS was formerly referred to as Enterprise Information Management (EIM).

2. Collaboration within AFMC and with our warfighting partners is critical to our timely delivery of systems and materiel. AFMC has selected EIS to facilitate this collaboration. EIS is being used for Headquarters staff meetings, Commander's Action Group operations, and for Command-wide forums like the recent AFMC Senior Leadership Conferences. I expect full adoption across this Command's Centers and bases, and full compliance to the EIS business rules, standards, and governance. All organizational sites should already be in full use, and each unit should be working with the EIS Program Management Office on functional sites.

3. The AFMC EIS direction is:

a. EIS is our office automation provider.

b. The AFMC enterprise standard EIS user interface is built on Microsoft Office SharePoint. The only authorized use of SharePoint in AFMC is on the AFMC EIS platform. Approval by HQ AFMC/A6/7 is required in order to add other tools that are not currently part of the standard AF EIS architecture. To view the AFMC authorized tools list, see the Knowledge Base at the following URL:
<https://cs.eis.afmc.af.mil/sites/eisusersupport/eimsupportcenter/FAQ/EIM%20Standard%20Tools%20List.aspx>.

c. AFMC organizations are prohibited from purchasing or installing SharePoint outside the AFMC EIS. Waivers to this policy must be requested from A6/7 and will be awarded on a very limited basis.

d. New EIS-like efforts, such as the purchase of commercial software, government off-the-shelf technology, or local development efforts are specifically prohibited.

e. Organizations with current efforts that duplicate EIS capabilities will develop and execute migration plans to move the existing capabilities to EIS or will provide a Business Case Analysis (BCA) that proves a financial benefit to AFMC to remain in the current capability. The organization will submit either the migration plan or the BCA to HQ AFMC/A6XI. Legacy systems will continue to operate until like functionality is provided within EIS. Air Force Knowledge Now (AFKN) and the AF Portal are exempt from this migration requirement and will continue to provide capabilities as described in Reference a.


f. Each of the tools should be used as described below:

- (1) Use EIS for AFMC internal office automation capabilities (document management, business process automation, collaboration, and enterprise information search).
- (2) Use AFKN for AFMC external collaboration and knowledge management. Once the EIS extranet is widely available, both EIS and AFKN can be used for external collaboration.
- (3) Use the AF Portal for static content to be shared across the AF or broader audiences.

g. For records management, AFMC organizations will continue to follow Reference b.

4. This guidance memorandum is provided in advance of the AFMC Instruction 33-XXX, Vol 1 and Vol 2, *AFMC Enterprise Information Services (EIS)* and *AFMC Enterprise Information Services (EIM)* respectively.

5. My POC is Mr. Gary Smith, HQ AFMC/A6XI, gary.smith2@wpafb.af.mil, DSN 674-0444, (937) 904-0444.


DONALD J. HOFFMAN
General, USAF
Commander

Attachments:

1. SAF/XC Memo, 21 Nov 08
2. AF ERM Solution, 4 Sep 07

Attachment 4

SAMPLE APPOINTMENT LETTER UNIT/ORGANIZATIONAL LETTERHEAD

Figure A4.1. Sample Appointment Letter Unit/Organizational Letterhead.

Date												
FROM: Unit/Organizational Commander (Portal Content Manager) OR 2 or 3 letter directorate/division chief (Portal Content Publisher) (Choose one option)												
TO: 88 CS/SCOKW												
SUBJ: Air Force Portal Content Manger/Publisher Appointment Letter												
1. The following named personnel are appointed (AF Portal Content Manager or Publisher, Choose Only One) to perform the duties of this position.												
Portal URL: _____												
<table border="1"> <thead> <tr> <th><u>NAME</u></th> <th><u>RANK</u></th> <th><u>OFFICE SYM</u></th> <th><u>DUTY PHONE</u></th> </tr> </thead> <tbody> <tr> <td><u>Primary</u></td> <td></td> <td></td> <td></td> </tr> <tr> <td><u>Alternate</u></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	<u>NAME</u>	<u>RANK</u>	<u>OFFICE SYM</u>	<u>DUTY PHONE</u>	<u>Primary</u>				<u>Alternate</u>			
<u>NAME</u>	<u>RANK</u>	<u>OFFICE SYM</u>	<u>DUTY PHONE</u>									
<u>Primary</u>												
<u>Alternate</u>												
2. The above named personnel have received the technical training required for the position. (Complete Training for New Content Managers) https://www.my.af.mil/gcss-af/USAF/ep/globalTab.do?channelPageId=sA4057E1F290AE3E80129367B34060462&programId=tA4057E1F2C393DCF012C5001778900B0												
Signature block Unit/Organizational Commander												
Attachments: training verification												

Attachment 5

**INTERNET RELEASE PACKAGE (IRP) FOR PORTAL WEB PAGE
COORDINATION/ APPROVAL****Figure A5.1. Internet Release Package (Irp) For Portal Web Page Coordination/Approval.****Page Path:****Date:**

Section I: Portal pages must meet the following requirements for posting information on private sites: (If No, explain on reverse). The paragraph references listed below refer to sections within WRIGHTPATTERSONAFBI 33-301.

1. Comply with copyright restrictions.**2. Pages contain accurate/current information. (3.2.2.2.3.)****a. On top level page:**

- 1) Content Manager's (CM) organization, office symbol, commercial phone number, and DSN. (3.2.2.2.2.1.)
- 2) organizational email addresses. (3.2.2.2.2.2.)
- 3) date last reviewed (pages/links must be reviewed at least every 180 days). (3.2.2.2.2.2.)

b. No empty portlets, topics, or content and no pages with "Under Construction"**3. Links are recently validated.**

External links are to be reviewed quarterly to ensure continued suitability (3.2.2.2.2.1.) and all pages/links are to be reviewed at least every 180 days. (3.2.2.2.2.2.)

4. Review process for portal pages includes (3.2.2.2.1.1.)

- a. OPSEC Office (to be consulted when the possibility of information becoming sensitive when aggregated with other non-sensitive information exists)
- b. Privacy Act Office (refer to paragraphs 12.1. and 12.2. of AFI 33-332 for releasable information and information that requires written consent).
- c. Office Foreign Disclosure (optional review depending on type of information)
- d. Legal (optional review depending on type of information)
- e. Contracting (optional review depending on type of information)
- f. Information Security Manager
- g. Unit Commander or equivalent

5. Pages are not used to promote personal/commercial gain, or endorse commercial products or service.

- a. Product endorsements or preferential treatment on official DoD Web sites is prohibited
- b. Use disclaimer when displaying commercial advertisements, sponsorships, or linking to nongovernment sites.
 - 1) No action required by CMs – this is part of the portal level disclaimer linked on every page.
 - 2) Commercial advertising and product endorsement are prohibited.
 - 3) Reproducing the contents of base newspapers for the Web is permitted if that content meets the restrictions provided.

6. Pages do not contain, link to, or promote obscene/offensive material.

Unauthorized storing, processing, displaying, sending, or otherwise transmitting offensive or obscene language or material. Offensive material includes, but is not limited to, “hate literature” such as racist literature, materials or symbols; sexually harassing materials, pornography and other sexually explicit materials.

7. Pages do not store/process classified material or critical indicator on non-approved systems.

Storing or processing classified information on any system not approved for classified processing.

8. Pages do not violate vendors’ license agreements.

- a. Obtaining, installing, copying, storing, or using software in violation of the appropriate vendor’s license agreement.
- b. Using graphics and artwork. Take great care when adapting existing artwork for use on Internet projects. Most licenses for software designed to prepare documents or briefings do not permit using the graphics for other purposes.

9. Pages are not copies of other sources on the Internet.

Information should remain as closely controlled by the source as possible to ensure its currency and accuracy. Do not copy files from other sources on the Internet and place them on a home page. Reference this information rather than repeat it.

10. Prevent users’ access to websites that are organizationally restricted. (3.2.2.2.1.2.)

If pages are restricted to organizations, for example, a disclaimer explicitly stating “Organizational access only” must be included (i.e. links to command SharePoint or Livelink sites).

11. If applicable, is DOD contractor proprietary information password and ID protected?

12. Pages do not display OPSEC material.

Critical information (sensitive mission data that by itself is unclassified, but when combined with other available data, may reveal classified information) is not displayed or linked on this page. The information has been reviewed for OPSEC releasability.

13. Pages comply with Privacy Act requirements. (3.2.4.)

- a. Do not post personal information on Private Web pages unless it is mission essential, falls under one of the Privacy Act exceptions for disclosing to third parties without consent of the subject, and appropriate safeguards are established. Add appropriate Privacy Act Statements or Privacy Advisories to pages that collect personally-identifying information and personal information from the subject (individual) that is filed in a Privacy Act system of record.
- b. If names and/or e-mail addresses are posted, has the local commander authorized posting and risk assessment been accomplished?

14. Pages Comply with 29 U.S.C. § 794d, Rehabilitation Act of 1998, Section 508, as amended by Public Law (PL) 105-220, Workforce Investment Act of 1998. (3.2.2.3.)

- a. Images and links must have alternate text.
- b. Videos that do not have close caption capability require transcript instead.

Section II: This certifies that this Web page complies with WRIGHTPATTERSONAFBI 33-301. (Electronically Sign or Print Name and Sign below):

Content Manager **Signature** (Required):

Information Provider/Content Owner **Signature** (Required):

Information Security Manager **Signature** (Required):

Freedom of Info Act/Privacy Act Mgr **Signature** (Required):

Staff Judge Advocate **Signature** (If applicable):

Foreign Disclosure Office **Signature** (If applicable):

Base Contracting **Signature** (If applicable):

Unit Commander (approval authority) **Signature** (Required):

Attachment 6

SAMPLE EIM/SHAREPOINT SITE OWNER APPOINTMENT LETTER

Figure A6.1. Sample EIM/Sharepoint Site Owner Appointment Letter.

printed on UNIT/ORGANIZATIONAL LETTERHEAD

Date

FROM: Unit/Organization

TO: 88 CS/SCOKW

SUBJ: EIM/SharePoint Top Level Site Owners

1. The following named personnel are appointed as *your org/office* EIM/Sharepoint Top Level Site Owners to perform the duties of this position.

NAMERANKOFFICE SYMDUTY PHONE

Primary:

Alternate:

Organization(s)/Site Name(s) serviced, list all:

2. The above named personnel have visited the **EIM Support Center:** <https://cs.eis.afmc.af.mil/sites/KnowOps/WPAFB/WebTeam/SharePoint%20Site%20Creation%20Documentation/SL%20EIM%20Support%20Center.aspx> to familiarize themselves with SharePoint and completed at least one of the following training options.

The self paced AFMC EIM Site Owner Training on the **AFMC EIM Site Owner Training Site:** <https://cs.eis.afmc.af.mil/sites/KnowOps/WPAFB/WebTeam/SharePoint%20Site%20Creation%20Documentation/SL%20AFMC%20EIM%20Site%20Owner%20Training%20Site.aspx>. (Attach verification of training).

Classroom Site Owner training course offered by the **WPAFB Training Delivery Element:** <https://cs.eis.afmc.af.mil/sites/KnowOps/WPAFB/WebTeam/SharePoint%20Site%20Creation%20Documentation/SL%20WPAFB%20Training%20Delivery%20Element.aspx>.

(Attach verification of training).

3. This letter supersedes all previous appointment letters. POC is

Signature block
Unit/Organizational Commander

Attachments: Training Verification