

**BY ORDER OF THE COMMANDER
SPECIAL OPERATIONS COMMAND**

**AIR FORCE SPECIAL OPERATIONS
COMMAND INSTRUCTION 33-303**



5 FEBRUARY 2015

Communications and Information

AFSOC PORTALS

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: AFSOC/A6OK

Certified by: HQ AFSOC/A6O
(Lt Col Elbert L. Coleman)

Supersedes: AFSOCI33-303,
14 January 2010

Pages: 10

This instruction implements guidance from Air Force Policy Directive (AFPD) 33-3, *Information Management*. This instruction implements the standard use of the Air Force Special Operations Command (AFSOC) Portals and identifies areas of responsibility for users at all levels. This instruction enforces United States Special Operations Command (USSOCOM) guidance and contains AFSOC policies and governance for the AFSOC Portals hosted on the secure internet protocol router network (SIPRNET), as well as non-secure internet protocol router network (NIPRNET). This instruction applies to all Air Force military, civilian, and contractor personnel under contract by Department of Defense (DOD), who develop, acquire, deliver, use, operate, or manage AFSOC Portals. This instruction applies to the Air National Guard (ANG) and the Air Force Reserve Command (AFRC) units using AFSOC Portal applications hosted by AFSOC. The term major command (MAJCOM), when used in this publication, includes field operating agencies (FOA) and direct reporting units (DRU.) **Failure to observe the prohibitions and mandatory provisions of this instruction by military personnel is a violation of the Uniform Code of Military Justice (UCMJ), Article 92; Failure to Obey Order or Regulation. Violations by ANG military personnel may subject members to prosecution under their respective State Military Code or result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contractor personnel will be handled according to local laws and the terms of the contract.** The authorities to waive wing/unit level requirements in this publication are identified with a Tier (“T-0, T-1, T-2, T-3”) number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, for a description of the authorities associated

with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items.

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). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the Air Force (AF) Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional's chain of command. This publication may be supplemented at any level, but all direct supplements must be routed to the OPR of this publication for coordination prior to certification and approval

SUMMARY OF CHANGES

This document has been substantially revised and must be completely reviewed. This document has been updated with tiering requirements of AFI 33-360; also updated AFSOC guidance and policies.

Chapter 1

AFSOC PORTALS POLICY AND GUIDANCE

1.1. Introduction. The AFSOC Commander's highest priority is to provide a Secure Operating Environment (SOE) to our warfighters. The AFSOC Portal technology is a secure asynchronous collaboration tool that will effectively and efficiently allow users to store data and share knowledge and information. The AFSOC Portals maintain a robust, collaborative environment ideal for the migration and automation of business processes. The portal capabilities support all AFSOC personnel in the creation, management, maintenance, sharing, disposition, and preservation of informational aspects of Air Force (AF) missions, operational support, and business processes. The AFSOC Portals provide a web-based entry point to the AFSOC knowledge base, allowing collaboration and knowledge fusion within and across organization boundaries. With support of AFSOC/A6, users will fulfill individual responsibilities involving training, shared drive cleanup, restriction of shared drives, migration of data, and sustainment of AFSOC's collaborative environment.

1.2. Purpose. This document defines the policy for the implementation and employment of the AFSOC Portals and its capabilities. The current portal technology capabilities include Workflow/Process Automation, Document Management, Records Management, Content Management, and Asynchronous Collaboration. This instruction applies to all Air Force military, civilian, and contractor personnel under contract by DOD, who develop, acquire, deliver, use, operate, or manage AFSOC Portals and should be interpreted as guidance for expected use of the portals in dissemination of Commander's critical information. This is not a how-to manual; rather, it provides guidance for the expected use and sustainment of Portal sites and dashboards. Refer to AFSOCPAM 33-304, *AFSOC Portals Guide for Site Owners and End Users*, for setup and management of the Portal sites. This document applies and refers to AFSOC Portals on NIPRNET and on SIPRNET.

1.3. Goals. The goals of the AFSOC Portals are to improve our interoperability with USSOCOM and United States Air Force (USAF); increase the efficiency of our core business processes; enhance the command's operations security (OPSEC) posture; to build command-wide collaboration and promote effective knowledge management in AFSOC.

1.3.1. Implement collaborative environment as a part of the SOE and USAF Enterprise Information Environment (EIE).

1.3.2. Transform our daily business and operational processes from current platforms (i.e., shared drives, functional systems, access databases) to the AFSOC Portals, while improving project, knowledge, and information management.

1.3.3. Provide a reach-back capability to allow forward deployed units to either push or pull documents through the AFSOC Portal capability, thus embracing the practice of information sharing as the norm, instead of the exception.

1.3.4. Provide a structure for data and information management to ensure information is visible, available and usable when and where needed to accelerate warfighter decision making and support deployed and in-garrison activities.

1.4. Assumptions.

1.4.1. The same rules for proprietary data, Privacy Act information, “For Official Use Only” and classified information still apply.

1.4.2. Paper records will continue to coexist with electronic records for the foreseeable future.

1.4.3. The integrity of electronic records must be maintained throughout their life cycle. Final records must be read only.

1.4.4. The current portals are currently NOT a records management solution. Users should continue to use the R: Drive, Electronic Records Management Drive, to store final records according to the approved file plan. The Air Force is currently developing an electronic records management solution. Separate guidance and an announcement will be disseminated at a later date.

1.4.5. Records Professionals (Functional Area Records Managers, Records Custodian) will periodically conduct inspections of organization filing practices (regardless of the storage media) and ensure data records are stored as appropriate. **(T-3)**

1.4.6. System security is a requirement for the individual. AFSOC will follow Air Force Instruction (AFI) 33-200, *Information Assurance Management*, and will not maintain classified information in an unclassified environment. **(T-0)**

Chapter 2

AFSOC ORGANIZATIONAL ROLES AND RESPONSIBILITIES

2.1. General. Implementation of the AFSOC Portals requires strong leadership, thorough education, and change management programs. Leadership support is required, at all levels of the MAJCOM, to continuously promote, support and set the example of incorporating information and knowledge sharing in day-to-day operations. If users are unwilling to share, portals immediately become ineffective and synchronization no longer takes precedence—adversely affecting the warfighters.

2.2. AFSOC Commanders and Directors should:

2.2.1. Direct migration of mission and business processes to AFSOC Portals to the maximum extent possible as applicable.

2.2.2. Encourage maximum utilization of leadership dashboards and portal environments.

2.2.3. Direct users to attend available training.

2.3. AFSOC Commanders and Directors will:

2.3.1. Appoint unit Primary and Alternate Site Owners in writing to perform site owner responsibilities. **(T-3)**

2.3.2. Hold end users personally accountable for improper marking and securing of classified information and PII on any site collection. **(T-0)**

2.4. AFSOC Communication and Information Directorate should:

2.4.1. Manage program operations command wide.

2.4.2. Provide governance and guidance to deliver robust collaborative mission capabilities through requirements analysis of mission needs.

2.4.3. Oversee development, deployment, and execution of site owner/end user training and user support materials.

2.4.4. Develop and issue relevant documentation, plans, and procedures to execute program components.

2.4.5. Report performance to AFSOC/CC using metrics (i.e., Portal Statistics Site) to assess implementation and effectiveness.

2.4.6. Manage and track central portal requirements and implementation.

2.4.7. Perform life-cycle management for the AFSOC Portals.

2.4.8. Execute change management, outreach and marketing for AFSOC Portals.

2.4.9. Provide training for base Knowledge Management cells to aide in the support of AFSOC portals.

2.5. AFSOC Communications Squadron and Flights will:

2.5.1. Act as the lead for the wing and group portal deployment and implementation. **(T-3)**

2.5.2. Manage program operations wing wide, to include:

2.5.2.1. Create and maintain a base Knowledge Management Cell comprised of Knowledge Management professionals to support all base users in the development and maintenance of the AFSOC portals. **(T-3)**

2.5.2.2. Oversee development, deployment, and execution of site owner/end user training and user support mechanisms. **(T-3)**

2.5.2.3. Execute change management, outreach, and marketing for AFSOC Portals on the base. **(T-3)**

2.5.2.4. Report performance, training completions and other program status updates to AFSOC/A6 using specified metrics and tools to assess implementation and effectiveness. **(T-3)**

2.5.2.5. Enforce all policy and guidance. **(T-3)**

2.5.2.6. Conduct Site Owner meetings to provide training and disseminate program information and updates to base unit representatives. **(T-3)**

2.6. Unit Site Owners will:

2.6.1. Perform all duties as specified in the appointment letter and should follow best practices in AFSOCPAM 33-304, *AFSOC Portals Guide for Site Owners and End Users*. **(T-3)**

2.6.2. Establish and maintain user permissions, which includes Visitors, Site Members, and Site Owner levels of permissions to the AFSOC Portals for their respective sites. **(T-3)**

2.6.3. Assist the AFSOC Portal Team and base Knowledge Management Cells in collecting information in relation to the administration and management of their sites as requested. **(T-3)**

2.6.4. Review information accuracy and validate site usage on a quarterly basis. **(T-3)**

2.6.5. Ensure all site content within AFSOC Portals are marked and protected with the appropriate classification and markings in accordance with AFI 31-401, *Information Security Program Management*, AFI 33-332, *Privacy Act Program*, and as established in the AFSOCPAM 33- 304. **(T-0)**

2.6.6. Assist end users in locking down personal identifying information (PII) content and manage access to the PII content as established in the AFSOCPAM 33-304. **(T-3)**

2.7. End Users should:

2.7.1. Attend end users training and any other available training to use the AFSOC Portals.

2.7.2. Use standard naming conventions as established in the AFSOCPAM 33-304.

2.7.3. Migrate business and operational processes to AFSOC Portals per direction of AFSOC/CC, as applicable.

2.7.4. Maintain data, information, and knowledge sharing within the AFSOC Portals.

2.7.5. Comply with tactics, techniques, and procedures (TTPs) as specified in AFSOCPAM 33-304.

2.8. End Users will:

2.8.1. Mark, secure and protect all documents and content containing PII and classified material in accordance with AFI 33-332, AFI 31-401, and AFSOCPAM 33-304. **(T-0)**

ANTHONY J. THOMAS, Colonel, USAF
Director, Communications and Information

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFPD 33-3, *Information Management*, 8 September 2011

AFI 31-401, *Information Security Program Management*, 1 November 2005

AFI 33-200, *Information Assurance Management*, 23 December 2008

AFI 33-332, *Privacy Act Program*, 5 June 2013

AFI 33-360, *Publications and Forms Management*, 25 September 2013

AFMAN 33-363, *Management of Records*, 1 March 2008

AFSOCPAM 33-304, *AFSOC Portals Guide for Site Owners and End Users*, in draft

Prescribed Forms

No forms are prescribed in this publication.

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AD—Active Directory

AF—Air Force

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRC—Air Force Reserve Command

AFRIMS—Air Force Records Information Management System

AFSOC—Air Force Special Operations Command

AFSOCI—Air Force Special Operations Command Instruction

AFSOCPAM—Air Force Special Operations Command Pamphlet

ANG—Air National Guard

DOD—Department of Defense

DRU—Direct Reporting Units

EIE—Enterprise Information Environment

EIM—Enterprise Information Management

FOA—Field Operating Agencies

IAW—In Accordance With

MAJCOM—Major Command
NIPRNET—Non-Secure Internet Protocol Router Network
OPR—Office of Primary Responsibility
OPSEC—Operations Security
PII—Personal Identifying Information
RDS—Records Disposition Schedule
RMA—Records Management Application
SPIRR—SharePoint Interim Records Repository
SIPRNET—Secure Internet Protocol Router Network
SOFNET—Special Operations Forces Network
SOE—Secure Operating Environment
TTP—Tactics Techniques and Procedures
UCMJ—Uniform Code of Military Justice
USAF—United States Air Force
USSOCOM—United States Special Operations Command

Terms

Business Processes—Concept of shepherding work items through a multi-step process. The items are identified and tracked as they move through each step, with either specified people or applications processing the information.

Capability—The ability to achieve an effect to a standard under specified conditions through multiple combinations of means and ways to perform a set of tasks.

Data—Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. For example, any representations such as characters or an analog quantity that is or might be assigned.

Document Management—The process of managing documents through their life cycle, from inception through creation, review, storage, dissemination, and archival or deletion. Document management can also be a database system to organize stored documents, or a search mechanism to quickly find specific documents.

Information—(1) Facts, data, or instructions in any medium or form. (2) The meaning that a human assigns to data by means of the known conventions used in their representation.

Information Management (IM)—The planning, budgeting, manipulating, and controlling of information throughout its life cycle (OMB Circular A-130).

Knowledge—Data and information that have been analyzed to provide meaning and value. Knowledge is various pieces of the processed data and information that have been integrated through the lens of understanding to begin building a picture of the situation.

Knowledge Management (KM)—(1) Systematic process of discovering, selecting, organizing, distilling, sharing, developing, and using information in a social domain context to improve warfighter effectiveness. (2) The governing and facilitation of knowledge activities (create, organize, formalize, distribute, apply, and evolve) within an organization in order to achieve its goals and objectives.