Department of the Army
Headquarters, US Army
Sustainment Command
1 Rock Island Arsenal
Rock Island, IL 61299-6500

*ASC Regulation 25-2

JUN 15 2017

Information Management

MANAGEMENT OF ARMY SUSTAINMENT COMMAND PUBLICLY ACCESSIBLE WEBSITES

Applicability. This regulation applies to all US Army Sustainment Command headquarters organizations and installations.

Supplementation. Supplementation of this regulation is authorized.

Proponent. The Deputy Chief of Staff for Information Management, G-6, is the proponent. Send comments and recommendations to Headquarters, US Army Sustainment Command, ATTN: AMSAS-IM, 1 Rock Island Arsenal, Rock Island, IL, 61299-6500, or click on the "Contact Us" link on the web Site itself (http://www.aschq.army.mil/home/).

Distribution. This publication is approved for electronic distribution from https://asc.aep.army.mil/sites/G6/g6staff/Records/Pages/Documents.aspx

Superseded Publications*. ASC 25-2, Mar 09.

FOR THE COMMANDER:

Official:

EARL B. SCHONBERG
Lieutenant Colonel, GS
Chief of Staff

Contents

Contents (cont.) Paragraph Page

1. Purpose. This regulation delineates the policy, provides guidance, and assigns responsibility related to establishing, operating, and maintaining ASC publicly accessible web sites.

2. References.

a. AR 25-1, Army Information Management Program.

b. AR 25-55, Army Freedom of Information Act Program.

c. AR 360-1, The Public Affairs Program.

d. AR 380-5, Department of the Army Information Security Program.

e. ASC Regulation 360-1, Public Affairs.

f. DoD Directive 8910.1 Management and Control of Information Requirements.

g. Production Web Code Update Policy, Document No. POL-50-10-00080 https://it.ria.army.mil/download.aspx?policyid=20, May 5, 2014.

h. Public Law 100-235, Computer Security Act of 1987.

i. Installation Campus Area Network (ICAN) and Classified Installation Campus Area Network (C-ICAN) System and Information Integrity Standard Operating Procedure (SII-SOP) #PRO-12-15-00183 Version 1.1 08/22/2016 https://it.ria.army.mil/download.aspx?policyid=103

j. Link to OPSEC training http://cdsetrain.dtic.mil/opsec/story.html

3. Abbreviations and Terms.

a. Publicly Accessible Web Site. A web site that contains releasable information and is accessible to the general public over the Internet. For the purposes of this regulation, the terms “publicly accessible web site” and “Internet web site” are synonymous.

b. Webmaster. The individual responsible for ensuring the posting of cleared material on a web server. This person is the single POC for all issues associated with the web server.

4. Policies.

a. It is fully appropriate for ASC organizations to establish and maintain publicly accessible web sites, provided they support legitimate, mission-related activities of the Army and are consistent with prudent operational and security considerations.

b. Consistent with other leadership responsibilities for public communication, the decision whether or not to establish an organizational web site and to publish appropriate instructions and regulations for a web site within limitations established by this regulation, is hereby delegated to each ASC organization. For the purposes of this regulation, an ASC organization is an HQ ASC directorate, special staff office, project team, or ASC subordinate unit.

c. Web page content must be suitable for audiences that may include non-military viewers. Ensure that information residing on a server with an "army.mil" domain cannot be interpreted as reflecting official Department of the Army (DA) policies or positions. Ensure that the information posted is consistent with official policies and positions.

d. Each organization operating a publicly accessible web site will implement technical security best practices with regard to its establishment, maintenance, and administration.

e. All ASC publicly accessible web sites will be DA-accredited and registered with appropriate agencies. All DA organizations are required to register their publicly accessible web sites, web publications, FOIA electronic reading room documents, and library sources in accordance with the Government Information Locator Service (GILS). The ASC G-6 (AMSAS-IM) and the Public and Congressional Affairs Office (AMSAS-PA) will register the ASC Home Page with GILS. HQ organization sites within the "aschq.army.mil" domain are included in the registration of the ASC Home Page. Installations must register their sites separately.

f. Ensure that all information is current, accurate, factual, related to the mission of the command organization, and

professionally presented. Ensure the page does not contain duplicate information existing elsewhere within ASC publicly accessible sites or information that is the responsibility of another organization or installation.

g. HQ ASC directors/chiefs and ASC unit commanders must ensure that information provided on any of their information sites does not contain classified or Privacy Act information, or information that could enable the recipient to infer classified or unclassified sensitive information, either from individual segments of the information or from the aggregate of information available. It is the commander's discretion to authorize, deny, or terminate organization web sites based on the sites ability to provide a value-added service, its enhancement of the organization's mission, or to realize efficiencies.

h. Publicly accessible web sites CANNOT contain items identifying employees' spouses, their children, or other personal identifying information. Do not use personal photos or post individual office telephone numbers. A statement such as “individuals in this office can be reached at (give a single office phone number)” may be used.

i. Obtain the owner’s permission when reproducing, distributing, or publicly performing copyrighted materials.

j. All web pages must be reviewed by the Public and Congressional Affairs Office (AMSAS-PA) before posting.

k. Web pages and their content are also subject to G-3 Operations Center (AMSAS-OPO), OPSEC Officer reviews.

l. The design of all web pages will conform to the Federal Information Technology Accessibility Standards (Section 508). The design of web pages will conform to the Army Content Online Resource Enterprise (CORE) Site Design Standards.

m. Links to other web sites.

(1) Links to civilian or military organizations, and programs and projects related to the mission and function of the organization, are authorized.

(a) Software download links to non-DoD sources and commercially (licensed) software are not allowed.

(b) Links to pages that support political views are not allowed. They give the appearance that the ASC is endorsing a particular political faction or viewpoint.

(c) The military, including ASC organizations, cannot endorse a product, organization, or exercise any responsibility over the contents at the destination pointed to by a link.

(d) Display the following disclaimer when linking to non-DoD sites. This disclaimer may appear on the page(s) listing external links or through an intermediate "exit notice" page generated by the server whenever a request is made for any site outside of the official information service (usually the .mil domain).

"The appearance of these hyperlinks does not constitute endorsement by the Army Sustainment Command (ASC) of these Web sites or the information, products or services contained therein. For other than authorized activities such as military exchanges and Morale, Welfare and Recreation sites, the ASC does not exercise any editorial control over the information you may find at these locations. These links are provided consistent with the stated purposes of this military Web site."

(e) Graphics or logos depicting commercial companies or products will not appear on ASC publicly accessible web sites.

(2) Review all external links periodically to ensure their continued suitability and availability. Remove all questionable or objectionable links.

n. Official Army Web information services cannot offer commercial sponsorships, advertisements, and endorsements. Commanders will ensure that association with commercial sponsorships, advertisements or endorsements does not adversely affect the credibility of official information.

o. Forms, Information Collection, and Usage Statistics.

(1) As a management function, evaluation of site usage data (log files) is a valuable way to evaluate the effectiveness of web information services. Collection of data such as the most or least requested documents, type of browser software used to access the web information service, etc., is appropriate. Collected data must be destroyed in 2 years, unless otherwise directed.

(2) Reference 2h, DoD Web Site Administration Policies and Procedures, 25 Nov 98, prohibited methods of collecting user-identifying information such as extensive lists of previously visited sites, e-mail addresses, or other information to identify or build profiles on individual visitors from the public. "Cookies" may be used with other methods to collect non-user identifying information to customize user sessions; however, notify users in advance of what and why information will be collected and how it will be used.

p. Web browser software.

(1) The standard browser is defined by the current Army Gold Master Image.

(2) Use and distribution of any software must comply with the applicable software licensing restrictions and agreements on Internet Index Server (IIS).

q. Public Web Server information will be stored in an individually segmented host environment. This segment will not be used to store anything other than publicly releasable information, even in areas or directories which are not shared to the internet.

5. Responsibilities.

a. The ASC Public and Congressional Affairs Officer (AMSAS-PA) will:

(1) Establish a process for the identification of information appropriate for posting to publicly accessible web sites and ensure it is consistently applied.

(2) Ensure the review of information for security, levels of sensitivity, and other concerns before release.

(3) Ensure the accuracy, consistency, appropriateness, and timeliness of all information placed on the web site.

(4) Conduct annual review of all HQ ASC and subordinate sites for compliance with established Public Affairs (PA) guidance for appropriateness of information. AMSAS-PA will notify the webmaster and page proponent(s) of any non-compliant information.

(5) Ensure the establishment of procedures for management oversight and regular functional reviews of the web site.

(6) For each employee publishing information on the ASC Public Web site, OPSEC certification is mandatory and must be updated annually. See references for link to training.

b. The G-3 Operations Center (AMSAS-OPO), OPSEC Officer will review information to ensure that information placed on publicly accessible web sites is appropriate for worldwide dissemination and does not place national security, DoD personnel and assets, mission effectiveness, or the privacy of individuals at an unacceptable level of risk.

(1) Each OPSEC Officer will be OPSEC certified, certification must be updated annually. See reference for link to training.

c. G-6 (AMSAS-IM), will:

(1) Provide policy and procedural guidance with respect to establishing, operating, and maintaining ASC websites.

(2) Approve and publish instructions and publications, as necessary, to guide, direct, or help ASC publicly accessible web site activities.

(3) Establish architectural and infrastructure guidelines for ASC web servers and user access to the hardware and software.

(4) OPSEC certification is mandatory and must be updated annually. See references for link to training.

d. Information Assurance Manager (IAM) (AMSAS-IM) will:

(1) Ensure Internet users are aware of the Internet’s vulnerabilities; their individual responsibilities; limitations of access; and the approval process for release of US Government information.

(2) Ensure the use of approved DOD security and privacy notices and applicable disclaimers on all web sites under their purview.

(3) Ensure that a comprehensive, multi-disciplinary security assessment is conducted of their web sites within 120 days of the promulgation of this document and at least annually thereafter.

(4) Ensure compliance with this policy for those functions, missions, agencies, and activities in their purview.

(5) Maintain the operational integrity and security of the computer and the network supporting the web site reference j, NEC policy and procedures, 03 Feb 17.

e. Webmaster will:

(1) Monitor professional appearance of web pages.

(2) Establish procedures for updates to web site content.

f. The ASC developer will enter tickets to affect changes to the public web following protocols set forth by the NEC-RIA (see paragraph 5g below).

g. The Network Enterprise Center - Rock Island Arsenal (NEC-RIA) will:

(1) Apply updates to the web provided by ASC WEB Developer per Production Web Code Update Policy, Document No. POL-50-10-00080, available at https://it.ria.army.mil/download.aspx?policyid=20. Service Request Management (SRM) tickets will be entered per their policy and a follow up email will be sent from ASC's Development POC that include the Incident number or the Request number to ensure the request is received before 1500hr deadline. The SRM request must include items delineated in the POL 50-10-00080.

(2) During the updating process, the NEC scans the code for 508 compliancy.

(3) Code updates are performed at 0900hrs on Monday - Friday (except for Federal Holidays). The customer POC will be notified upon completion.

(4) ASC Development POCs must provide a confirmation of site functionality within 2 hours of receiving notification that the website has been updated or the ticket will be closed. If the site is not functioning correctly, the customer can request a rollback of the site (ref. 2.3.2 POL-50-10-00080).

(5) NEC-RIA will also perform security scans and maintenance as set forth in the Installation Campus Area Network (ICAN) and Classified Installation Campus Area Network (C-ICAN) System and Information Integrity Standard Operating Procedure (SII-SOP) #PRO-12-15-00183 Version 1.1 08/22/2016 https://it.ria.army.mil/download.aspx?policyid=103

h. HQ ASC directors/chiefs and ASC subordinate commanders, or their designated representative, will:

(1) Establish procedures to ensure that classified, Privacy Act information, or information that could enable the recipient to infer classified or unclassified sensitive information, from individual segments of the information, or from the aggregate of the information, is not posted to ASC publicly accessible web sites and that classified information is not transmitted to the Internet.

(2) Establish procedures for the periodic review of newsgroups, bulletin boards, and web pages maintained by their offices to ensure the postings do not adversely affect the ASC.

i. Content providers will take responsibility for periodically reviewing and making sure their web pages conform to this guidance. Reviews will be completed semiannually.

Appendix A
Taskmaster Process Flow Chart