

Guidance for Management of Publicly Accessible U.S. Army Websites

30 November 1998

New: Army Operations Security OPSEC [checklist](#) is available online! (1/29/99)

SUBJECT: Guidance for Management of Publicly Accessible U.S. Army Websites

1. Purpose.

- . This memorandum provides guidance for the establishment and operation of publicly accessible, non-restricted, U.S. Army World Wide Web (WWW) websites (Army websites). Publicly accessible, non-restricted Army websites will only provide information that has been properly cleared for release.
- b. The World Wide Web is an efficient and effective means for the U.S. Army to share information. Army websites should focus on providing value-added information services and products to the organization's users, customers, the Army, and the public through the sharing of accurate, timely, and relevant information. To ensure that the Army fully leverages the capabilities of the WWW in a manner that is efficient, focused on saving resources, and moving toward a digital environment, the following guidance is provided.

2. Proponent and exception authority.

- . The proponent for this memorandum is the Director of Information Systems for Command Control, Communications, and Computers (DISC4).
- b. The DISC4 has the authority to approve exceptions to this memorandum that are consistent with controlling law and regulation. The DISC4 may delegate the authority to approve exceptions to this policy, in writing, to a division chief under his supervision within the proponent agency that holds the grade of Colonel or GM/GS-15.

3. References.

- . This policy supersedes Director of Information Systems for Command, Control, Communications, and Computers 301404Z October 1996 Guidance for the Management of Army Websites.
- b. 5 USC Chapter 35, "Paperwork Reduction Act", as amended.

- c. Public Law 100-235, Computer Security Act of 1986.
- d. For guidance on use of government-owned computing equipment and resources (e.g., non-duty related email use and web browsing in the workplace), see DoD 5500.7-R, Joint Ethics Regulation (JER), 30 August 1993 and Change 2, 25 March 1996.
- e. For all DoD newspapers, including electronic publications, DoD Instruction 5120.4, DoD Newspapers and Civilian Enterprise Publications, May 29, 1996 applies.
- f. For image manipulation standards, DoD Directive 5040.5, Alteration of Official DoD Imagery, August 29, 1995 applies.
- g. AR 25-1, The Army Information Resource Management Program (25 March 1997).
- h. AR 25-55, Army Freedom of Information Act Program (10 January 1990).
- i. For access-controlled websites, AR 380-19, Information System Security (1 August 1990) applies.
- j. AR 340-21, Army Privacy Act Program (5 July 1985).
- k. AR 360-5, Public Information (31 May 1989).
- l. AR 380-5, Department of the Army Information Security Program (25 February 1988).
- m. AR 530-1, Operational Security (3 March 1995).
- n. HTML 3.2 Reference Specification, World Wide Web Consortium (W3C) Recommendation, 11 January 1997.
- o. HTML 4.0 Specification, World Wide Web Consortium (W3C) Recommendation, 24 April 1998.

4. Definitions and explanation of abbreviations.

- a. WWW - world wide web
- b. HTML - hypertext markup language
- c. W3C - World Wide Web Consortium
- d. CGI - common gateway interface
- e. GILS - Government Information Locator Service
- f. FOUO - for official use only
- g. FOIA - Freedom of Information Act
- h. MACOM - major command
- i. GO/SES - general officer/senior executive
- j. DoD - Department of Defense
- k. Webpage - an individual HTML-compliant electronic file accessible through a TCP/IP network
- l. TCP/IP network - a data communication network that uses transport control protocol/internet protocol (TCP/IP); the public internet and the DoD Non-classified IP Router Network (NIPRNET) are examples of TCP/IP networks

- m. Website - a collection of HTML-compliant electronic files designed to provide information, services, or goods to users through a TCP/IP network
- n. Homepage - the single, top-level, webpage designed to be the first file accessed by a user visiting a website; also known as an "index" or "default" page

5. Responsibilities.

- . The leader of each organization that operates an official U.S. Army website (leadership), regardless of location or echelon (e.g., unit, office, installation, major command), will:
 - 1. exercise ultimate control over the content of the organization's website,
 - 2. define the purpose of the website in terms of how it supports the mission of the organization,
 - 3. define the core functions, products, and information that will be made available through the organization's website,
 - 4. ensure compliance with all applicable policies, including AR 530-1, Operational Security (3 March 1995), and
 - 5. periodically reevaluate each website under their control to ensure performance of the responsibilities in paragraphs 5.a.(1) through 5.a.(4).
- b. The organization's leadership may delegate the execution of this responsibility to one or more website managers and other appropriate officials. Where appropriate, the organization's leadership may delegate these responsibilities to a team of subject matter experts, the exact composition of which is left to the discretion of the leadership. This team may be composed of subject matter experts from one or more of the following communities: Public Affairs, Communications/Computers, Intelligence, Legal, and others.

6. Policy.

- . Specifications and Standards.
 - 1. Official U.S. Army websites should be implemented in such a way as to support the widest range of potential users and computing platforms. Use of non-standard or proprietary website elements will not benefit the widest range of potential users.
 - 2. For hypertext markup language (HTML) documents, official U.S. Army websites must use any of the HTML specifications listed by the World Wide Web Consortium (W3C). As an alternative, official U.S. Army websites may employ any HTML specification that is a W3C Proposed Recommendation, or any non-HTML specification that is a W3C Recommendation. W3C Technical Reports (including Recommendations and Proposed Recommendations) are found online at <http://www.w3.org/TR/>.
 - 3. Official U.S. Army websites may employ non-standard (e.g., browser-specific) HTML tags and browser extensions (plug-in). However, official U.S. Army websites

may not require or encourage users to use any particular browser product or "plug-in" technologies. Official U.S. Army websites may not be designed to support any particular browser product.

b. Requirements for Organizations Operating Websites.

1. Every Army organization that maintains a website must register it with the U.S. Army Homepage through the online registration form found on the U.S. Army Homepage [</register/>](#).
2. Every Army organization that maintains a website must notify the U.S. Army Homepage Webmaster <mailto:webmaster@hqda.army.mil> when the universal resource locator (URL) or any of the point of contact information required as part of the registration process changes.
3. Every Army organization that maintains a website must register it with the Government Information Locator Service (GILS) <http://www.dtic.mil/index/>
4. Every Army organization that maintains a website must display a Privacy and Security Notice.
5. U.S. Army organizations operating an official website will provide the following information or hyperlinks to the following information on their homepage:
 - a. Organization missions and functions.
 - b. Organizational structure, listing or hyperlinking to parent and subordinate command or organization websites. Organizational charts containing individuals' names and other personal information should not be made available to the public unless privacy and security concerns have been addressed; posting such information for members of deployable units and others in sensitive positions could make them potential targets of hostile organizations or individuals.
 - c. Electronic mail address, phone number, or mail address of the point of contact responsible for the website content.
 - d. A hyperlink to the U.S. Army Homepage <http://www.army.mil>.

c. Requirements for Website Managers. A website manager is the organizations' leader, or an individual or group that has been delegated the following responsibilities by the organization's leadership. Website Managers (webmasters) will:

1. Ensure that information published on their website is accurate, timely, represents the official Army position, and is properly cleared for public dissemination;
2. Ensure appropriate security and access controls are in place, commensurate with the perceived threats, and to ensure that the following types of information is not made available to unauthorized individuals or organizations:
 - a. Classified
 - b. Unclassified but sensitive
 - c. Information that cannot be disclosed under the Privacy Act
 - d. For Official Use Only (FOUO)
 - e. Freedom of Information Act (FOIA)-exempt information (including, but not

limited to draft policies and regulations, and pre-decisional information)

- f. Copyrighted information for which releases from the copyright owner have not been obtained
3. Provide the highest practicable level of assurance that information made available to or received from the public does not contain malicious software code (e.g., viruses, trojan horses), or if it does, to sufficiently notify the user before the download of such information begins;
4. Respond to email, direct queries to the appropriate source of information, or otherwise fulfill or redirect requests for information;
5. Ensure that the organization's website provides point of contact information for the webmaster.
- d. Requirements for Webpages. All U.S. Army webpages will display the date when that page was last updated, reviewed, or cleared for public release.
- e. Release of Information.
 1. The organization's leadership will institute a review process to ensure that information provided on their website(s) is current, timely, and cleared for public release. The organization's leadership is responsible for the release of all information on the organization's website.
 2. The following types of information will not be made available to the public through the WWW:
 - . Classified
 - b. Unclassified but sensitive
 - c. Information that cannot be disclosed under the Privacy Act
 - d. For Official Use Only (FOUO)
 - e. Freedom of Information Act (FOIA)-exempt information (e.g., draft policies and regulations, or pre-decisional information)
 - f. Copyrighted information for which releases from the copyright owner have not been obtained
 3. Commanders of Army major commands (MACOM Commander), or equivalent, may authorize a waiver to the restrictions at paragraphs 6.e.(2) and 6c.(2) for draft doctrinal and draft technical information only. The ability to waive this prohibition may not be delegated below the GO/SES-level in the MACOM Headquarters. To authorize a waiver in such cases, a MACOM Commander (or the delegated MACOM Headquarters authority) must:
 - . Sign a memorandum waiving the prohibition against releasing draft doctrinal or draft technical information to the public.
 - b. Addresses the intelligence and national security, public affairs, legal, and contractual issues pertinent to the public release of the draft doctrinal or draft technical information to the public.
- f. Commercial Advertising and Sponsorship.
 1. Commercial advertising on official U.S. Army websites is prohibited. Corporate or

product logos and trademarks (other than text or hyperlinked text) are considered commercial advertisements, and may not be served from official U.S. Army websites.

2. No money, services, products, or in-kind payment (e.g., website hosting, site management, site design) will be accepted in exchange for a link to a non-Army web resources placed on an official U.S. Army website.
3. No product endorsement will be served from an official U.S. Army website. Official U.S. Army websites will not provide preferential treatment to non-U.S. Government entities.

g. External Linked Content.

The ability to hyperlink to resources external to the Army is a fundamental feature of the World Wide Web, and can add value and functionality to Army websites.

1. Hyperlinks to web resources other than official U.S. Army (non-Army) web resources are permitted if the organization's leadership certifies them to be in support the organization's mission.
2. Official U.S. Army websites may use only text or hyperlinked text to direct users to non-Army software download sites.
3. Army websites that provide links to non-Army web resources must display a disclaimer in accordance with DoD policy.

h. Collection of Information. Army websites that collect standardized information from 10 or more members of the public must comply with:

1. DoD Memorandum, *Web Site Administration Policies and Procedures*, 25 November 1998 <http://www.defenselink.mil/admin/dod_web_policy_12071998.html#part1>.
2. The Paperwork Reduction Act of 1995 (as amended).

i. Personal Use.

1. Personal use of government resources generally is improper.
2. Hyperlinks on Army websites to homepages, websites, or other web resources of a personal and non-mission related nature are prohibited.
3. Army Internet users are subject to DoD 5500.7-R, change 2, Joint Ethics Regulation (JER), 25 Mar 1996.

j. Restricted Access.

1. In addition to not posting certain information to Army websites as noted above in paragraph 6.e., webmasters shall ensure that Army websites do not provide direct hyperlinks (or other methods to bypass access-controls, such as hyperlinking to webpages below password protection webpages) to the following types of information:

- a. Classified
- b. Unclassified but sensitive
- c. Information that cannot be disclosed under the Privacy Act
- d. For Official Use Only (FOUO)
- e. Freedom of Information Act (FOIA)-exempt information (including, but not

limited to draft policies and regulations, and pre-decisional information)

- f. Copyrighted information for which releases from the copyright owner have not been obtained
2. Publicly accessible Army websites may provide hyperlinks to access-controlled websites only through intervening access-control mechanisms or procedures that are sufficient to address the perceived level of threat and sensitivity of the information.
3. Army websites must not use inflammatory or threatening language when describing access-controls and procedures, and must avoid the perception that the Army is hiding or withholding information that otherwise would be available to the public.

7. Point of contact.

- . Point of contact for this policy is the Army Homepage Webmaster, <mailto:webmaster@hqda.army.mil>.

-
-  [to u.s. army homepage](#)
 -  [security & privacy notice](#)
 -  last update: 01061999