

**BY ORDER OF THE COMMANDER  
AIR UNIVERSITY (AETC)**



**AIR FORCE INSTRUCTION 33-129**

**AIR UNIVERSITY SUPPLEMENT 1**

**13 NOVEMBER 2003**

**Communications and Information**

**TRANSMISSION OF INFORMATION VIA THE INTERNET**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the Maxwell Electronic Publications web page at: <http://www.maxwell.af.mil/msd/pubs/library.htm>. If you lack access, contact the Publications Management office.

---

OPR: HQ AU/SCXP  
(Mr Wayne Glass)  
Supersedes AFI 33-129/AUS1, 12 Feb 02

Certified by: HQ AU/SCXP  
(Ms Marietta Magaw)  
Pages: 4  
Distribution: F

---

**AFI 33-129, 4 April 2001, is supplemented as follows:**

This supplement implements AFI 33-129, *Transmission of Information Via the Internet*. This information applies to Air University (AU), 42d Air Base Wing (ABW) and tenant organizations. The use of the name or mark of any specific manufacturer, commercial product, commodity or service in this publication does not imply endorsement by the Air Force or Air University.

### **SUMMARY OF REVISIONS**

This revision adds additional guidance on web page compliance (paragraph 4.2.1.10). A star (★) indicates changes since previous edition.

3.5. Scholarly works and AU student papers are subject to special security and policy review before publication. Public Affairs (HQ AU/PAS) provides guidance for releasing scholarly, scientific and student research papers via the Internet.

3.6.5. (Added) (AU) Organizational commanders are responsible for the accuracy of information posted to their organizational pages and determining the appropriate levels of protection to afford this information. (See also paragraph, 7.5 this supplement).

3.6.6. (Added) (AU) Commanders have responsibility for ensuring links from their organizational pages to other pages are consistent with the professional image of the Air Force.

3.8.1. The local Air Force Network Control Center (AFNCC), MSD/ITI, is responsible for defending the base network against unauthorized access. For security purposes, the AFNCC monitors traffic through the base Internet gateway and may deny incoming traffic (FTP, telnet, gopher, HTTP) not addressed to registered Internet servers.

4.1. MSD/IT will appoint a Web Administrator who will act as the primary web server administrator for all AU schools (less AFIT) and 42d ABW organizations. Organizations with web sites not residing on a Maxwell server will assist with functional administration of their server.

4.1.1.6. All web servers on Maxwell AFB are registered with the local AFNCC, MSD/ITI.

4.2.1.2. Information providers have primary responsibility for obtaining and documenting release authorization for information placed on the organizational home page. At the organization's request, the public affairs office (PA) assists in reviewing the information product and recommending the appropriate degree of releasability. Page maintainers should verify release authorization before posting information to the page. (See also paragraph, 7.5 this supplement).

4.2.1.3. All opening pages of posted documents (such as the table of contents of a book or first screen of a multimedia presentation) contain a link back to the organizational home page. All organization home pages link back to the AU home page.

4.2.1.7. Page maintainers institute internal procedures to ensure posted information remains current. One method to facilitate this requirement is for all information to reflect a date of posting. This date provides viewers a reference as to the currency of the data displayed.

4.2.1.9. (Added) (AU) Section 508 of the Rehabilitation Act Amendments of 1998 requires Federal information technology be equally accessible to both disabled and non disabled Federal employees and members of the public; therefore, all web sites must comply with this statute. Specifically, all new web sites will be built according to Section 508 guidelines. All existing web sites should comply at their next major revision. Contact the Maxwell Web Administrator if you need further clarification on Section 508 compliance issues.

★4.2.1.10. (Added) (AU) Web page maintainers will be notified when pages are not compliant with current DoD directives, AFIs and AF-CIO policy memorandums. The Web page maintainer will have 15 calendar-days from the date notified to bring the page in compliance. If the page continues to be noncompliant, the commander of the organization will be notified, and the page will be deactivated until it meets compliance.

4.2.1.10.1. Items prohibited on publicly accessible Web pages:

4.2.1.10.1.1. Personally identifying E-mail addresses (except on .mil restricted sites)

4.2.1.10.1.2. Individual photographs (those not associated with authorized, official biographies)

4.2.1.10.1.3. Group photographs

4.2.1.10.1.4. Telephone directories/rosters

4.2.1.10.1.5. Individual names (except on .mil restricted sites)

4.2.1.10.1.6. Detailed base map graphics which identify building locations and streets.

4.2.1.10.1.7. Itineraries or agendas which disclose travel dates, times, and visit locations for distinguished visitors.

4.2.1.10.2. Use of personally identifying information will be authorized on a case-by-case basis. Air University Public Affairs will be the approval authority for variances. Rationale may include:

4.2.1.10.2.1. Biographies: Deputy Wing commander or equivalent and above are the only authorized official Air Force biographies. No other biographies are authorized.

4.2.1.10.2.2. Faculty vitae: Short descriptions of faculty qualifications and expertise are permissible.

5. (Added) (AU) The Maxwell AFB Web Administrator maintains the Air University World Wide Web server. Organizations with a new requirement to place information on a web server must contact the Maxwell AFB Web Administrator for guidance on developing pages. The Maxwell AFB Web Administrator allocates organizations space on its server and grants page maintainers remote access to their organizational data to perform maintenance.

6.1.5. Organizations may use AU Form 879, **Copyright Reprint Permission Request and Reply**, or a suitable letter to document reproduction permission from the copyright holder. The Staff Judge Advocate can assist in recommending appropriate wording for the request.

6.1.13. (Added) (AU) **Use of Streaming Audio and Video.** Individuals and organizations are permitted to access streaming audio and video for those activities essential to the day-to-day accomplishment of their mission. Users will coordinate with the Information Protection Office (42 CS/SCSI) to allow this mission-essential information onto the base network.

6.4. Type 2 and Type 3 private organizations are not authorized to use government computing services or equipment to establish or maintain WWW sites or Internet servers but may be entitled to support from the AU home page for information dissemination. Refer to AFI 34-223, *Private Organization (PO) Program*, for guidelines covering private organizations.

7.3.1. Limited access information should clearly state any release restrictions in the body of the file; for example, FOUO in the header or footer of a text file. This precludes inadvertent downloading and retransmission of limited access information to unauthorized personnel.

7.5. Organizations create Internet Release Packages using AU Form 38, **Internet Release Authorization**, to document the review, coordination and release approval of information products released via the Internet. Generally, information intended for public release is subject

to stricter review than limited access information. AU schools will use the AU Research Work Releasability Checklist to document the review, coordination and release approval of information products released via Internet of student papers.

11.1.2.3.5. (Added) (AU) Another threat to our automated environment is a computer hoax. Attackers originate rumors of a new virus or malicious program in hope others spread the rumor and disrupt an organization's normal computing activity. Reports of computer viruses should be verified with organizational Computer Security Managers and reported to the Wing Information Protection Office (IPO). If a genuine threat exists, the IPO is OPR for notifying organizations of the threat and appropriate precautionary measures.

19. (Added) (AU) **Forms Prescribed.** AU Form 38, **Internet Release Authorization**, and AU Form 879, **Copyright Reprint Permission Request and Reply.**

MARK S. WINTERSOLE, Lt Col, USAF  
Director, Communications and Information