5 FAM 730
SYSTEM SECURITY

(CT:IM-92;   08-01-2007)
(Office of Origin: IRM/BPC/PRG)

5 FAM 731 SYSTEM SECURITY

(CT:IM-59;   04-14-2005)

a. Network administrators must work closely with Information Systems Security Officers (ISSOs) to ensure the effective implementation of Department computer security policy.

b. Internet and intranet servers must be treated as sensitive and protected accordingly. Department computer security policies apply to all Intranet servers.

c. Access to a server, specific directories, and to specific Web pages that require limited access should be restricted based on User IDs and passwords. Department computer security policies apply to Web servers. Refer to 12 FAM 623.3, Accountability.

d. System managers must keep anti-virus software updated, anti-virus definitions current, and implement any anti-virus plug-ins for the browser. Anti-virus definitions are available on the intranet.

   For offices unable to access the intranet, contact the IRM Systems Integrity Division, IRM/OPS/ITI/SI. Do not use the Internet to perform definition updates, except on standalone PCs. All new files to be added to a server must be scanned by anti-virus software. Department of State policies governing the use of unauthorized software must be rigorously enforced (see 5 FAM 841.4 paragraph c). New software must be run in a test environment until it is deemed safe to install on a live system.

e. Department Web sites, whether managed by IRM, or managed internally within a bureau or office, must conform to Department computer security requirements outlined in 12 FAM 600 Information Security Technology. ISSOs and Web site managers are responsible for implementing the Department’s security policy.

   Bureaus that use customized Web-enabled applications, whether created internally or by a contractor, (e.g., Java applications and applets, CGI, Perl scripts) must work with DS/CIS/IST to ensure that the applications are appropriately secure prior to implementation.

f. Security audits must be carried out regularly, along with a risk assessment to identify and quantify all potential threats and exposures. Internet security must be aggressive and proactive. Robust security involves three types of measures:

(1) Protective—physical access control and/or encryption;

(2) Validation-oriented—active probing and compliance testing; and

(3) Audit reviews and monitoring—audit trails, policy breach detection, and activity monitoring.

Contact DS's Evaluation and Audit Branch (DS/CIS/IST/ACD/EAB) for information relating to security audits.

g. The posting on any Internet Web site, or discussion in any chat room or any other public forum on the Internet, of classified or Sensitive But Unclassified (SBU) information is strictly prohibited. (See 12 FAM 540 for an in-depth definition of SBU information.)

h. Classified foreign government information (FGI) that is subject to modified handling rules may be processed on the Department's unclassified AIS and transmitted via the Internet if such transmission is explicitly authorized by the originating government or governing international agency, or by a relevant agreement, obligation, or handling policy.

i. The items below are provided as minimum security guidelines for Web sites hosted by external commercial Internet service providers (ISP). The Department recognizes that not all ISPs can meet these recommendations. Posts should, however, work with the ISP to make the site as secure as possible.

(1) The following are ISP responsibilities that will be established with the ISP by the local Web site manager. They will be verified by the ISSO:

(a) The hosting ISP has a security policy and provides a copy to the mission. Have the ISSO examine it for reasonability, not necessarily adherence to 12 FAM requirements, but providing a reasonable degree of protection;

(b) The hosting ISP has a firewall or other, comparable security configuration measures in place to protect against hacking.

The site manager should check with DS/CIS/IST/ACD for acceptable alternatives to a firewall;

(c) The hosting ISP has been security-certified by a professional organization;

(d) The hosting ISP has a program in place for managing current software patches;

(e) The hosting ISP has anti-virus software installed and virus signatures are updated routinely;

(f) Where possible, Web pages should be hosted on a dedicated server not accessible to the ISP's other clients. Set Web pages to read only, with provisions for authenticated, authorized U.S. Government personnel to have remote access, as needed, for a limited period of time during the day to maintain the site content; and

(g) The hosting ISP should sign a written agreement with the senior official responsible for the site, typically the PAO, which outlines the Department's security expectations with respect to the integrity and availability of the Web pages hosted by the ISP.

(2) Site managers are responsible to:

(a) Establish 24-hour emergency procedures to contact the ISP, and vice-versa, in the event of an incident. Ensure these procedures include a method for authenticating the caller, and that they are not dependent on services, e.g., e-mail that may have been compromised as part of the incident;

(b) Domestically work with the ISP to ensure that non-resident aliens do not have direct or indirect operational access to Department Web pages;

(c) Archive Web pages every time they are changed officially, and do not rely solely on the ISP;

(d) Monitor Web pages daily for unauthorized changes;

(e) Limit the use of JavaScript and similar scripting languages to avoid known vulnerabilities these tools present; and

(f) Perform frequent, periodic overwrites of data, to ensure prompt restoration in the event of unauthorized changes.

5 FAM 732 THROUGH 739 UNASSIGNED