5 FAM 820

INFORMATION TECHNOLOGY ROLES AND RESPONSIBILITIES FOR SYSTEM OPERATIONS/MANAGEMENT

(CT:IM-151; 07-16-2014)
(Office of Origin: IRM/BMP/GRP/GP)

5 FAM 821 GENERAL

(CT:IM-50; 05-04-2004)

This section defines responsibilities for system operations and management. See also 5 FAM 120, 12 FAM 622, and 12 FAM 630.

5 FAM 822 CHIEF INFORMATION OFFICER

(CT:IM-151; 07-16-2014)

The CIO:

1. Is the Department’s senior Information Technology professional. The CIO reports via the Under Secretary for Management to the Secretary of State on all matters relating to information resource management;

2. Ensures availability of information technology systems and operations, including IT contingency planning, to support the Department’s diplomatic, consular, and management operations;

3. Ensures that appropriate procedures are in place for system authorization of national security systems;

4. Serves as the Designated Approval Authority (DAA) for non-Special Compartmented Information (non-SCI) systems in the Department; and

5. Is the Department official responsible for compliance with the Paperwork Reduction Act, 44 U.S.C. §3501 et seq; implementation has been delegated to the Bureau of Administration, Office of Directives Management, A/GIS/DIR (see Delegation of Authority 226, dated October 13, 1998).
5 FAM 823  CHIEF INFORMATION SECURITY OFFICER (CISO)

(CT:IM-115; 04-25-2011)

The CISO:

1. Reports directly to the CIO on all matters pertaining to IT security;
2. Develops and maintains the Department’s information security program;
3. Provides guidance to personnel with responsibilities for information security and coordinates with information systems security officers (ISSOs) domestically and abroad; and
4. Coordinates the design and implementation of processes and practices that assess and quantify risk.

5 FAM 824  INFORMATION SYSTEMS SECURITY OFFICER (ISSO)

(CT:IM-151; 07-16-2014)

The ISSO:

1. Ensures that the systems for which they are responsible are configured, operated, maintained, and disposed of in accordance with all relevant IRM and DS security guidelines;
2. Is responsible for overseeing configuration and administration of auditing and for ensuring that audit trails are reviewed periodically and archived in accordance with security guidelines;
3. Works closely with IMO/ISO/System Administrator to ensure all security related functions and activities are performed;
4. Plays a leading role in introducing an appropriate methodology to help identify, evaluate, and minimize risks to all IT systems; and
5. Is responsible to the CISO to ensure that IT system is configured and maintained securely throughout its lifecycle in accordance with the Systems Security Plan (SSP). See also 12 FAM 620 and 12 FAM 630.

5 FAM 824.1  Domestic Information Systems Security Officer (DISSO)

(CT:IM-151; 07-16-2014)

The DISSO:

1. Provides desktop security support and fulfills “in-scope” information
systems security officer (ISSO) as defined in 1 FAM 275.4-3;

(2) Performs in-scope ISSO roles and responsibilities for domestic consolidated bureaus which include:

(a) Establishing enterprise policy, processes and procedures in compliance with DOS desktop security guidelines;
(b) Administrating access control/user accounts to include file permissions;
(c) Performing desktop incident handling to include incident response, computer incident response team's (CIRT) litigation and remediation requests;
(d) Executing desktop security audits to include random security scans;
(e) Managing software download request authorizations;
(f) Monitoring data transfer requests to include authorizing transfers to and from CDs, DVDs and other removable media;
(g) Providing training and education to include performing security briefings as well as informing users of Department of State security best practices; and
(h) **Responsibility** for maintaining requirements for all desktops and providing desktop security guidance to all users within bureaus that have fully consolidated—as defined by the respective master service level agreement (SLA) for each consolidated bureau and ISSO appointment memo.

(3) Works closely with “out-of-scope” ISSOs whose roles and responsibilities include:

(a) Performing certification and accreditation requirements;
(b) Managing “out-of-scope” applications and servers;
(c) Performing routine security audits for out-of-scope server functions; and
(d) Regulating physical security.

**5 FAM 825  SYSTEM OWNER**

*(CT:IM-151; 07-15-2014)*

a. Domestically, the system owner is the bureau-designated senior executive that is responsible for the system. Abroad, the system owner is the Chargé, deputy chief of mission, consul general, or principal Officer or equivalent, or the bureau-designated senior executive responsible for the system.

b. Each system owner:
(1) Is responsible and accountable for the business aspects of managing a system, including funding and representing the interests of the system throughout its lifecycle;

(2) Ensures adequate confidentiality, integrity, and availability of data and applications software residing on the system;

(3) Ensures system security plans and contingency plans are developed and maintained for each system and applications; and

(4) Ensures systems personnel are properly designated, and trained; and appoints the ISSO and the alternate ISSO for a system.

5 FAM 826 INFORMATION MANAGEMENT OFFICER (IMO)/INFORMATION SYSTEMS OFFICER (ISO)/SYSTEM ADMINISTRATOR

(CT:IM-115; 04-25-2011)

The IMO/ISO/system administrator:

(1) Develops and maintains system security plans and contingency plans for all IT systems and major applications for which he or she is responsible;

(2) Participates in risk assessments to periodically reevaluate sensitivity of the system, risks, and mitigation strategies; and

(3) Installs only hardware and/or software approved by the IT CCB or local CCB. See 5 FAM 120 for further information on the roles and responsibilities of personnel managing systems abroad.

5 FAM 827 USER

(CT:IM-151; 07-16-2014)

The user must:

(1) Adhere to Department guidelines governing the personal use of information systems;

(2) Not download, install, or use software on any Department computer without prior approval from the ISSO or ISSO’s delegated representative;

(3) Use e-mail systems in a professional and courteous manner with the understanding that misuse of Department e-mail will subject them to possible disciplinary action (see 12 FAM 642);

(4) Use properly formatted passwords and protect them from unauthorized disclosure. Unauthorized disclosure is the release of password information to persons other than senior IT management or security personnel for
purposes of performing an investigation; and

(5) Not use a system or application before receiving appropriate training.

5 FAM 828 ACTIVE DIRECTORY (AD) ACCOUNTS

5 FAM 828.1 Administration of Active Directory Accounts

(CT:IM-151; 07-16-2014)

a. This section provides guidance for system administrators on the administration of active directory (AD) accounts.

b. If the user is scheduled to be away from the office in excess of 90 days the following steps must be taken:

(1) Employee email and data files will be archived by the system administrator and the employee network user account will be deleted; and

(2) Upon return to duty, the employee’s network account will be recreated by the system administrator and email and data files will be restored from the archive. The normal account creation process applies.

c. If an AD user account is inactive over 90 days and determined to be inactive, and no guidance is received from the account holder, the account will be deleted.

5 FAM 828.2 Special Circumstances for Active Directory Accounts

(CT:IM-151; 07-16-2014)

a. Under special circumstances, there are legitimate reasons for an account to be unused for more than 90 days:

(1) Medical leave; or

(2) An unforeseen event (e.g., bereavement leave)

b. The "hold" organizational unit (OU) is site/post created active directory container for the temporary storage of inactive accounts. The hold OU must be configured in accordance to the "Department of State Global Address List (GAL) and Active Directory Standardization Guide."

c. No account will remain in the hold OU in excess of 180 days.

d. System administrators/ISSOs are responsible for the management of the hold OU.
5 FAM 828.3 Inactive Accounts

(CT:IM-151; 07-16-2014)

a. In order to manage accounts that are authorized to be inactive longer than 90 days, system administrators will:
   Relocate the accounts to a special site/post created “hold OU.”

b. Privileged accounts cannot reside in the Hold OU. All accounts placed in the site hold OU must include the following information in the account “Description” field:
   The system administrator will be sent the “Description” field for the Site\Owning Site Email Contact\Start Date (MM/DD/YYYY)\End Date (MM/DD/YYYY).

c. Accounts within the domain hold OU that do not contain the required information or that exceed the assigned “end date” will be subject to deletion.

e. Post and domestic ISSOs responsibilities remain as per 5 FAM 824) for user account oversight.

5 FAM 829 UNASSIGNED