United States Department of Agriculture
Research, Education, and Economics

ARS ❑ CSRESS ❑ ERS ❑ NASS

Policies and Procedures

Title: ARS Information Systems Security Program

Number: 253.3-ARS

Date: August 19, 1998

Originating Office: Information Technology Division, Network Operations Branch, AFM/ARS

This Replaces:

Distribution: ARS Headquarters, Areas, Locations

This P&P establishes the policy supporting program goals, and the assignment of responsibilities for the management, implementation, and operation of the ARS Information Systems Security Program.

Table of Contents

1. Authorities

The Privacy Act of 1974; Federal Managers Financial Integrity Act of 1983; PL 100-235, "The Computer Security Act of 1987;" OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems;" OMB Circular A-123, "Internal Control Systems;" OMB Circular A-127, "Financial Management Systems;" Departmental Regulation (DR) 3140-1, "USDA Information System Security (ISS) Policy."

2. Background

The use of distributed information systems to store, process, and communicate sensitive information and the integration of computer and telecommunication technologies have made information systems security more complex. The benefits of using this technology must be accompanied by the implementation of an information systems security program (ISSP) that reduces the associated security risks to an acceptable level.

3. Applicability

The policies and associated information systems security standards and guidelines will apply to all ARS organizational elements and to other components of USDA having data resident on ARS computer systems. They also apply to all other personnel who have responsibility for operating automated information systems of ARS or who have access to ARS data or equipment.

4. Information Systems Security Program Objectives

The objectives of the ARS ISSP are to:

- provide uniform policy and centralized guidance on information systems security;
- establish requirements for the protection of sensitive information against disclosure, modification, or destruction;
- protect information resources from fraud, theft, or misuse;
- maintain the continuity of ARS operations by preventing or minimizing the impact of events that interfere with normal information processing operations;
- ensure that security planning and risk management requirements are integrated into the ARS systems development process; and
- provide training to promote information systems security awareness and accountability at all levels within ARS.

5. Information Systems Security Program Elements

The ISSP is a balanced combination of management and staff actions, operational activities, and technological control measures. The following ISSP elements will be addressed in more detail in the forthcoming ARS Information Systems Security Manual, 253.3-ARS:

- **Policies, Standards, and Guidelines.** The foundation of the ISSP is the development and implementation of policies, standards, and guidelines in compliance with those at the Federal and departmental level.

- **Assignment of Security Responsibilities.** Managers will ensure that responsibilities for information systems security are clearly communicated to all employees. When required by the importance of the computer resources and/or the sensitivity of the information processed, an information systems security representative may be formally designated to exercise security management functions on behalf of the responsible manager.

- **Effective Use of Protective Technology.** ARS will make full use of available hardware, software, and communications security technology wherever cost effective to protect Agency information technology resources. New information technology systems will be reviewed to ensure that appropriate security is integrated into systems design.

- **Security Education and Training.** Education and training are key elements in the ISSP. Information systems managers, technical staff, and users will be familiar with the established goals and responsibilities of the ISSP. To accomplish this, ongoing security awareness and education training will be provided to all employees.

- **Risk Management.** ARS will, to the maximum extent feasible, implement a risk management program that ensures security risks are identified and evaluated and includes the development and maintenance of computer security plans, contingency plans, and certifications and accreditation of sensitive systems and applications.

- **Reviews.** ARS information systems will be afforded periodic security reviews as required by Federal regulations and Departmental Directives.

- **Contingency Planning.** The increased dependence on automated information systems makes it essential that plans and procedures be prepared and maintained to:

    - minimize the damage and disruption caused by undesirable events; and

    - provide for the continued performance of essential system functions and services.

- **Security Accreditation of Sensitive Information Applications.** A formal security accreditation process will be implemented to ensure that appropriate controls have been designed into sensitive computer applications. An essential feature of this process will be

the responsibility of management in the determination of control requirements and the assessment of the internal control environment for the application.

- **Protection.** ARS will establish appropriate safeguards and procedures to detect actual or potential security violations and to counteract each threat as identified in a risk analysis. The various types of security procedures will include the following:

    - Physical security practices that focus on required measures for protecting the structure housing automated information systems and related equipment from damage by accident, fire, or environmental hazards.

    - Personnel security practices that focus on procedures established to ensure that all personnel who have access to sensitive information have the required authorities and clearance.

    - Communications security practices that focus on required measures such as passwords, encryption, data authentication, and security software used to prevent unauthorized access to information or data resident on information systems or peripheral devices.

    - Equipment security practices that combine with physical security to ensure the protection of hardware components of a system.

    - Software and data security practices that focus on the protection of operating systems, applications software, and database files.

    - Administrative security practices that include those planning and procedural measures associated with the implementation and administration of the computer security program.

6. Policy

It is the policy of ARS to establish and maintain an effective ISSP that complies with applicable Federal and Department information systems security policies and addresses ARS requirements for confidentiality, integrity, and availability.

7. Summary of Responsibilities

ARS information systems security responsibilities are implemented through, but not limited to, the following:

Senior Information Resources Management Officer (SIRMO):

- Develops and maintains a cost effective ISSP that assures compliance with established Federal mandates and Department requirements.

- Implements the ISSP through the ARS ISSP Officer.

ISSP Officer

- Plans, develops, and directs a comprehensive ISSP.

- Monitors and reports on ARS compliance with Federal and Department information system security policies and standards.

- Oversees the development and implementation of ARS information system security goals and objectives.

- Develops, coordinates, implements, and maintains security policies, procedures, and guidelines for the protection of all ARS information sources.

- Designs and implements a comprehensive risk management program.

- Conducts periodic information systems security risk assessments and security reviews of operational or proposed automated information systems and computer facilities.

- Provides consolidated budgetary planning and review for information systems security equipment, training, control software, and services.

- Serves as the principal information systems security consultant to ARS components that use, develop, or operate automated information systems.

- Supports the goals and objectives of the Privacy Act of 1974 by establishing appropriate physical, systematic, and procedural safeguards to assure the confidentiality of personal information processed by ARS automated systems.

- Represents ARS at Department and other Federal Government organizations and specialized groups on information systems security activities.

- Issues standards for the development and maintenance of contingency plans for emergency response, backup operations, and post-disaster recovery of ARS information systems and facilities.

- Provides guidance to the Deputy Security Officers and all Security Points of Contact.

- Establishes criteria for computer security awareness and training and ensure that a security training program is implemented to meet the requirements of the Computer Security Act of 1987.

- Issues appropriate instructions needed to implement provisions of computer security policies and standards established in ARS Directives, Department Regulations, and Federal laws.

Deputy Administrators, Associate Deputy Administrators, Headquarters Staffs, Administrative Financial Management (AFM) Divisions, and Area Directors

- Appoint a Deputy Security Officer at each ARS Area.

- Implement established information security policies within their areas of responsibilities.

- Promote information systems security awareness and ethical use of automated information systems.

- Ensure appropriate security requirements are included in specification and contract documents for acquisition or operation of computer facilities, equipment, software packages, or related computer services.

- Promptly report to the ISSP Officer any breaches of security; events that may indicate security violations; or attempts to gain unauthorized access to computers, information systems, or data resident on information resources.

- Develop security plans for each general support system and major application identified in accordance with OMB Circular No. A-130, Appendix III, and OMB Bulletin 90-08 as a **minimum**. These plans are due to AFM/Information Technology Division (ITD) on March 1 of each year.

Area Administrative Officers, With Assistance from Location Coordinators

- Appoint a Security Point of Contact at each ARS location.

Area Deputy Security Officers

- Serve as the main contact point for Information Systems Security for their designated program area and as liaison between Security Points of Contact and the ISSP Officer.

- Implement computer security policies, procedures, and guidelines for the protection of information resources.

- Participate in the development of computer security plans and contingency plans as well as certifications and accreditation of sensitive systems and applications.

- Participate in risk assessments and periodic security reviews of operational or proposed automated information systems.

- Provide technical guidance to Security Points of Contact.

- Provide authorized users appropriate access to ARS applications, and to NFC and National Information Technology Center (NITC) remote-based applications following approval from respective Functional Managers.

Location Security Points of Contact

- Serve as primary security liaison with the Deputy Security Officers and ISSP Officer.

- Promptly report to the Deputy Security Officers any breaches of security; events that may indicate security violations; or attempts to gain unauthorized access to computers, information systems, or data resident on information resources.

All Users of Automated Information Systems

- Comply with all security requirements pertaining to the automated information resources they use.

- Practice good housekeeping with all computer equipment (i.e., computer areas should be uncluttered, and food, drinks, and smoking should be kept away from computers).

- Safeguard all user ID's and passwords to automated information systems.

- Backup data and systems on a regular basis.

- Understand and comply with all licensed software agreements before using the software at each work area.

- Report all computer security incidents to the Deputy Security Officer or ISSP Officer.

8. Glossary

Accreditation. Authorization and approval of a certified automated information system to process sensitive data.

Administrative Security. The security discipline which focuses on those planning and procedural measures associated with the implementation and administration of the computer security program.

ARS Security Requirements Committee. An ad hoc Information Security Committee designated by the SIRMO and determined by the security matter being addressed.

Automated Information System. The organized combination of ADP equipment, software, and established methods and procedures designed to collect, process, and communicate data or information supporting specific administrative, mission, or program requirements. This includes application systems, databases, and management information systems.

Automated Information Systems Security. The managerial, technical, and physical safeguards used to ensure the confidentiality, integrity, and availability of sensitive information processed by or transmitted through Federal automated information systems.

Certification. Technical evaluation of automated information systems, made as part of and in support of the accreditation process, that establishes the extent to which a particular automated information system or network design and implementation meet pre-specified security requirements.

Communications Security. The security implemented to ensure that only authorized users are able to access the system from a remote location.

Confidentiality. Ensuring that sensitive information is kept private and is accessible only by authorized personnel who have a need to know.

Data. A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by manual or automated means.

Equipment Security. The security of the hardware components of a system.

ID. User Identification Code

Information. Any communication or representation of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative maintained in any medium or form, including computerized databases, paper, microfilm, or magnetic tape.

Information System. The organized collection, processing, maintenance, transmission, and dissemination of information in accordance with defined procedures.

IRM. Information Resources Management

ISSP. Information Systems Security Program

ITD. Information Technology Division

NFC. National Finance Center

NITC. National Information Technology Center

OMB. Office of Management and Budget

Personnel Security. The procedures established to ensure that all personnel who have access to sensitive information have the required authorities and clearance.

Physical Security. Procedures required for the protection of the structures housing automated information systems and related equipment from damage by accident, fire, or environmental hazards.

Risk Analysis. An evaluation of automated information systems assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of these events. Identifies potential threats and their probability of occurrence and proposes safeguards to combat these threats.

Risk Management. The total process to identify, control, and minimize the impact of uncertain events. The process facilitates the management of security risks by each level of management throughout the system life cycle. The approval process consists of three elements: risk analysis, certification, and approval.

Sensitive Information. Information that requires protection because of the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect proprietary data, the ability of an agency to accomplish its mission, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act.

SIRMO. Senior Information Resources Management Officer. The designated official responsible for carrying out the IRM functions assigned to the Agency by the Paperwork Reduction Act. The Director of ITD is designated as the ARS SIRMO.

Software and Data Security. The security of operating systems software, applications software, and database files and the information they contain.

/s/

FLOYD P. HORN
Administrator
Agricultural Research Service