



United States
Department of
Agriculture

Farm
Service
Agency

Rural
Development

Natural
Resources
Conservation
Service

April 13, 2012

KS FAC NOTICE: 2012-03

TO: All Kansas Farm Service Agency (FSA), Natural Resources Conservation Service (NRCS), and Rural Development (RD) Offices

FROM: State Food and Agriculture Council (FAC)

SUBJECT: Automated Data Processing (ADP) and Visitor Log Implementation Guidance

BACKGROUND

Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), mandates that all federal agencies, develop, document and implement an agency-wide program to provide security for the information systems that support their operations and assets. FISMA requires agencies to adhere to guidance established by the National Institute of Standards and Technology (NIST).

Departmental Regulation (DR) 3505-003, Access Control Policy establishes the basis for implementing secure access control practices for protecting information systems and data within the United States Department of Agriculture (USDA). The policy requires USDA agencies to ensure access to all Information Technology (IT) systems complies with Federal Information Processing Standards (FIPS) and National Institute of Standards and Technology (NIST) Special Publication (SP) and Office of Management and Budget (OMB) Standards.

Departmental Manual (DM) 3510-001, Chapter 2, Part I, Physical Security Standards for Information Technology (IT) Restricted Space states: *A sign in/out logbook shall be required for all escorted visitors.*

FSA, NRCS, RD and International Technology Services (ITS) require security controls in worksites (buildings and facilities) to protect the confidentiality, integrity and availability of information and systems. Furthermore, they require: ***“visitor access to non-public areas of worksites must be restricted, logged and regularly reviewed. Visitors must be escorted while in non-public portions of worksite.”***

The Operations Security Branch (OSB) and ITS, Technical Support Division (TSD), have released Version 1.0 of the Security Standard Operating Procedures Guide, dated March 10, 2011. In this new release, Section 2.0 requires new regulations for the ADP room and in particular maintaining an access log, which follows the guidelines stated in DM 3510-001.

IMPLEMENTATION GUIDANCE:

For Offices that have a Secure ADP Room:

A Sign-In/Out Visitor Log **MUST** be utilized to record visitor entry and exit of the secure ADP room and the visitor **MUST** be escorted while in the secure ADP room. Visitor refers to anyone that does not have the proper means to unlock the secure ADP room via a key, cipher lock combination, proper key card access, etc.

Impact:

- a visitor (producer, service maintenance, technician, repair person, etc...) would ONLY be required to sign the secure ADP room log when allowed access into the secure ADP room
- service center personnel deemed to have proper means to unlock the secure ADP room would NOT be required to sign this log

For Offices that do not have a Secure ADP room:

A Sign-In/Out Visitor Log MUST be utilized to record visitor access to the non-public space of the service center office and the visitor MUST be escorted while in the non-public space. Instead of requiring the visitor to complete the log, the service center personnel MUST record the visitor information on the log. Visitor refers to anyone that does not have the proper authority to be in the non-public space. Non-public space is any space where ADP equipment resides.

Impact:

- a visitor (producer, service maintenance, technician, repair person, etc...) would ONLY be required to be recorded on the visitor log when allowed access to the non-public space
- a visitor is NOT required to sign the log; instead, the service center personnel would update the log with the visitor's information
- service center personnel deemed to have the proper authority to be in the non-public space would NOT be required to sign this log.

ADDITIONAL INFORMATION:

As a reminder, a secure ADP room is for IT and telecommunication equipment including the AS400. This room will be approximately 75 to 100 square feet. No storage of any kind is allowed in a secured ADP room. Do not store filing cabinets, storage boxes, or bookcases, etc. in this area. This is not a storage room. The door to the ADP room is to remain closed and locked at all times.

A sample **ADP Room Access Log** template is posted in the **Forms** folder on the TSD Internal SharePoint site. https://its.sc.egov.usda.gov/tsd/tsd_staff/default.aspx.

A copy of the ADP Room Access Log is included with this notice. Please post this Log at the appropriate location described above.

If you have any questions regarding this new policy, please contact your agency security officer.


ADRIAN POLANSKY
State Executive Director
Farm Service Agency


PATRICIA A. CLARK
State Director
Rural Development


ERIC B. BANKS
State Conservationist
Natural Resources
Conservation Service