APHIS ENTERPRISE DATA BACKUP POLICY

1. PURPOSE

This Directive establishes APHIS policy for enterprise data backup.

2. REFERENCES

a. National Institute of Standards and Technology (NIST) Special Publication 800-53 Recommended Security Controls for Federal Information Systems. http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf

b. Federal Information Systems Controls Audit Manual (FISCAM), Volume 1: Financial Statement Audits. http://www.gao.gov/special.pubs/ai12.19.6.pdfSCOPE

3. SCOPE

This Directive applies to the APHIS Enterprise Backup System and data backed-up by this system. This Directive does not apply to other systems, processes, or methods used to backup data in APHIS. This Directive does not apply to electronic documents that qualify as Federal records nor should it be assumed that the record retention for backup policies is in line with Federal records management guidelines. If an electronic document qualifies as a Federal record, the entire message must be printed out and filed in the appropriate paper file system per APHIS records management regulations (http://inside.aphis.usda.gov/records/emailrec.htm).

4. DEFINITIONS

a. Backup. An electronic, recoverable copy of data.

b. Enterprise Backup. The electronic, recoverable copy of data captured by and stored on an Agency backup system.

c. Enterprise Backup System. The combination of hardware and software used to perform enterprise backup and restoration of data.

d. Enterprise Server. A server that delivers functionality to APHIS employees or customers outside of a single region.

5. POLICY

Data loss can occur as a result of many causes, such as human error, natural disaster, carelessness, malicious acts, and catastrophic system malfunctions such as disk failures. Implementation of a backup system is an important and cost-effective method to protect Agency investments in data and software, and to ensure APHIS's continuing ability to meet mission goals. Reliable, systematic backup of critical data also plays an important role in enterprise disaster recovery plans and processes. Section 2.a. and b. provide recommended security controls for prevention of data loss through a managed backup strategy. This Directive establishes APHIS' policy and processes for the implementation of Section 2.a. and b. controls, as follows:

a. APHIS will implement and maintain an Enterprise Backup System to ensure the integrity, security, and availability of critical APHIS information, data, and software.

b. All data stored on enterprise servers will be backed-up via the APHIS enterprise backup system according to an established schedule commensurate with industry best practices and program requirements. The development of these requirements is the responsibility of program staffs in cooperation with APHIS, Marketing and Regulatory Programs (MRPBS), Information Technology Division (ITD). Current APHIS requirements for specific data type back-ups are as follows:

Frequency	Server	Retention
Daily	Mail	4 weeks
	File	4 weeks
	Database	4 weeks
Monthly	Mail	1 year
	File	1 year
	Database	1 year

In general, all database files are backed-up on a daily basis. Some individual databases are backed-up less frequently per program requirements.

c. Data stored on non-enterprise servers will be backed-up via the APHIS Enterprise Backup System by special request as capacity allows.

d. The media containing enterprise back-ups will be stored at offsite locations which are environmentally controlled and secure.

e. Enterprise Backup System logs will be monitored daily to confirm successful backup, and to promptly detect and correct Enterprise Backup System hardware, software, or configuration failures.

f. Agency management will regularly inspect Enterprise Backup System documentation and audit logs to confirm that regular back-ups are being performed, and records are being kept, in accordance with the terms of this Directive.

g. Documentation pertaining to the Enterprise Backup System, including backup logs, reports, and documentary evidence of offsite storage activities will be maintained until superseded or obsolete, in accordance with General Records Schedule 24, item 4b as stated below:

(1) "System Back-ups and Tape Library Records.

(2) Tape library records including automated files and manual records used to control the location, maintenance, and disposition of magnetic media in a tape library including list of holdings and control logs. Destroy/delete when superseded or obsolete."

6. RESPONSIBILITIES

a. The APHIS Chief Information Officer will:

(1) Approve and ensure implementation of this Directive.

(2) Approve any modifications to this Directive.

(3) Ensure that appropriate funding is available to support the activities required by this Directive.

b. Deputy Administrators/Directors of Program Units, and Heads of Major Business Offices will:

(1) Disseminate this Directive to their respective staffs.

(2) Ensure that the terms of this Directive are followed within their Program Units, and that appropriate procedures are developed, implemented, and monitored to implement the processes mandated by this Directive.

(3) Assist in promptly identifying, investigating, and rectifying violations of this Directive.

c. The Technical Resource Management (TRM) Manager, MRPBS, ITD, will:

(1) Maintain this Directive, including receiving requests for, and executing, modifications in response to change requests and/or new requirements.

(2) Perform a quarterly review of APHIS' Enterprise Backup System procedures and activities to ensure that the terms of this Directive are being followed.

(3) Inspect Enterprise Backup System records (e.g., backup logs, reports, evidentiary documentation of offsite storage activities, hardware and software maintenance records, and documentation of corrective actions) to ensure that records are maintained in compliance with the terms of this Directive.

(4) Review, approve, and sign reports of quarterly reviews of APHIS' Enterprise Backup System procedures and activities.

(5) Review and sign reports of corrective actions performed as a result of deviations identified during quarterly reviews.

(6) Ensure that deviations identified during quarterly reviews are corrected within 30 days.

d. The TRM, MRPBS, ITD Staff will:

(1) Manage the APHIS Enterprise Backup System in compliance with the terms of this Directive.

(2) Be responsible for all activities related to the configuration and maintenance of the APHIS Enterprise Backup System.

(3) Manage all activities related to the offsite storage of Enterprise Backup System media, including contract statements of work, recordkeeping and documentation, and monitoring vendor performance.

(4) Perform daily examinations of Enterprise Backup System logs to confirm successful backup, and detect any backup system failures or anomalies.

(5) Take immediate and appropriate action to investigate and correct Enterprise Backup System hardware, software, or configuration failures.

(6) Generate quarterly reports of Enterprise Backup System activities for signature by the TRM Manager, MRPBS, ITD. Documentation will include a summary of Enterprise Backup System activities, detected anomalies, a description of the resulting investigation(s) and results, and corrective actions taken.

(7) Be responsible for filing, maintenance, and disposal of all Enterprise Backup System documentation, including backup logs, reports, evidentiary documentation of offsite storage activities, hardware and software maintenance records, and documentation of corrective actions, per the terms of this Directive.

7. INQUIRIES

a. Questions concerning the information and processes described in this Directive should be directed to the Manager, MRPBS, ITD, TRM.

b. This Directive can be accessed at ***www.aphis.usda.gov/library***

/s/
Gregory L. Parham
APHIS Chief Information Officer