UC Riverside, School of Medicine Policies and Procedures
Policy Title: Enterprise Data Backup Policy
Policy Number: 950-02-226

Responsible Officer:	Information Security Officer
Responsible Office:	Compliance
Origination Date:	1/30/2018
Date of Revision:	N/A
Scope:	• All UCR School of Medicine (SOM) information, in its electronic form, regardless of where it resides, who possesses it or who has authority to create, store, transmit or use it; • All Technology Infrastructure owned and/or administered by UCR SOM; • All UCR SOM divisions, including those of UCR Health subsidiaries, if any; • All UCR SOM facilities, including those of UCR SOM subsidiaries, if any; and • All UCR SOM workforce members, including employees, interns, contractors, consultants, and vendors doing business with UCR SOM including any individuals affiliated with third parties that access UCR SOM systems.

I. Policy Summary

The purpose of this policy is to define UCR Health's requirements regarding backup and restore of enterprise information. This policy provides guidance to prevent against data loss and recover from power failure, data corruption, or an information security incident.

II. Definitions

Please refer to the Standard Definitions Guide.

III. Policy Text

UCR SOM will maintain and use a secure, efficient, and effective backup and restore process. All data stored on enterprise systems must follow these requirements.

IV. Procedures

A. Identification of Critical Data

UCR SOM must identify what data is most critical for its business. This can be done through a formal data classification process or through an informal review of information assets. If a formal data classification process is performed it will follow the *IS-3 Electronic Information Security Policy* method of identifying data in the format of P1-P4 based on the type of data. Regardless of method, critical data should be identified so that it can be given the highest priority during the backup process.

B. Data Types to Backup

Data will be backed up based on the importance to the business balanced with the burden the backup would place on users, network resources, and the backup administrator. Data to be backed up shall include, but is not limited to:

1. All data determined to be critical to UCR SOM operation and/or employee job function.
2. All patient data
3. All shared information stored on enterprise file servers
4. All mailboxes on the enterprise email server
5. All data classified as P3 or P4 according to the *IS-3 Electronic Information Security Policy*

Individual workstations are not backup up. It is the responsibility of the data owner to ensure any data of importance is moved to the file server or other authorized location.

C. Backup Frequency

Backup frequency is critical to successful recovery. The following backup schedule will allow for sufficient data recovery capability in the event of an incident, while avoiding an undue burden on the users, network, and backup administrator.

- Incremental backups performed daily
- Full backups performed weekly

D. Off-Site Retention

Geographic separation of backups from the source system must be maintained, to some degree, in order to protect from fire, flood, or other regional or large-scale catastrophes. Offsite storage must be balanced with the time required to recover the data, which must meet the uptime requirements of the source system. Backups should be rotated off-site at least once a month.

E. Backup Media Storage

Backup media must be stored in an access-controlled area. Online backups are allowable if the service meets the criteria specified in this policy.

Confidential data must be encrypted using industry-standard algorithms to protect UCR SOM against data loss.

If a secured media vault is used for backup storage, the backup administrator will place the backup media into the secured media vault at some agreed upon time (set in the backup procedures document and based on the criticality of the data being backup up) after successful completion on the backup. The secured media vault will meet fire and disaster standards for media and will be kept locked at all times. Only the backup administrator will have access to the secured media vault. In the event that the secured media vault is not available or properly functioning, the backup administrator will move backup media to a secured offsite location until the secured media vault becomes available.

F. Backup Retention

All backup retention will conform to UCR SOM data retention policy. Unless otherwise noted in the data retention policy, minimum backup retention will be as follows:

- Incremental backups must be saved for one week
- Full backups must be saved for one month

G. Restoration Testing

1. Backup restore testing must be performed at least twice annually, with a sufficient backup data set to have high confidence that backups and restoration is performing normally.
2. Backup restores must be tested when any change is made that may affect the backup system.

H. Backup Validation

The testing of the validity of backup data and the ability to restore data in the event of a computer system problem, failure, or other disaster shall occur at least monthly and more often is necessary to ensure integrity, confidentiality, and availability.

Successful restore functions shall be logged. Any problems identified during the restore function shall be acted upon immediately.

V. Responsibilities

OIT (Office of Information Technology) will be responsible for managing the daily operations of the backup system, which includes but is not limited to, the following:

1. Managing the daily and weekly incremental and full backups
2. Testing of the restoration process at least twice annually
3. Managing any logs of enterprise backups, including the date/time of backup and the priority of the data according to the *IS-3 Electronic Information Security Policy*
4. Documenting any backup errors and performing corrective actions appropriately
5. Validating the backup and restore functions are working properly
6. Backup infrastructure maintenance
7. Ensuring backups are rotated offsite as appropriate

Information Security Officer will be responsible for:

1. Reviewing backup and restore testing logs
2. Creating and updating risk assessments in relation to backups
3. Reviewing any exceptions to this policy

VI. References

UCOP IS-3 Electronic Information Security Policy

VII. Revision History

New policy

Approvals:

Compliance Committee 1-30-2018

Paul Hackman, J.D., L.LM., C.H.C.
Compliance and Privacy Officer,
School of Medicine

Deborah Deas, M.D., M.P.H
Dean, School of Medicine
CEO, Clinical Affairs