Policy Title: Information System Recovery and Reconstitution

Policy Type: Administrative


Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Recovery incorporates executing information system contingency plan activities to restore essential missions and business functions. Reconstitution takes place following recovery and includes activities for returning the information system to its original functional state before contingency plan activation.

TABLE OF CONTENTS

| Contacts | 1 |
| Stakeholder(s) | 1 |
| Purpose | 2 |
| Requirements | 2 |
| Violations | 3 |
| Interpretation | 3 |
| Publication | 3 |
| Review Schedule | 3 |
| Related Documents | 3 |

CONTACT(S)

Office of Information Technology – (757)823-2869
STAKEHOLDER(S)

University Faculty & Staff
Office of Information Technology

PURPOSE

This control establishes the University’s policy for recovery and reconstitution of University information systems in the event of hazardous occurrences that might result in disruption of normal operations.

REQUIREMENTS

NSU provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

Supplemental Guidance: Recovery and reconstitution procedures are based on University priorities, established recovery point/time and reconstitution objectives, and appropriate metrics. Reconstitution includes the deactivation of any interim information system capability that may have been needed during recovery operations. Reconstitution also includes an assessment of the fully restored information system capability, a potential system reauthorization and the necessary activities to prepare the system against another disruption, compromise, or failure. Recovery and reconstitution capabilities employed NSU can be a combination of automated mechanisms and manual procedures.

Controls Enhancement for Sensitive Systems:

1. The information system implements transaction recovery for systems that are transaction-based.

   Enhancement Supplemental Guidance: Database management systems and transaction processing systems are examples of information systems that are transaction-based. Transaction rollback and transaction journaling are examples of mechanisms supporting transaction recovery.

2. NSU provides compensating security controls for those University-defined circumstances that can inhibit recovery and reconstitution to a known state.

3. NSU provides the capability to reimage information system components within NSU-defined restoration time-periods from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.

VIOLATIONS
Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 32-01 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

INTERPRETATION

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.

PUBLICATION

This policy shall be widely published and distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

1. Communicate the policy in writing, electronic or otherwise, to the University community within 14 days of approval;
2. Submit the policy for inclusion in the online Policy Library within 14 days of approval;
3. Post the policy on the appropriate SharePoint Site and/or Website; and
4. Educate and train all stakeholders and appropriate audiences on the policy’s content, as necessary. Failure to meet the publication requirements does not invalidate this policy.

REVIEW SCHEDULE

- Next Scheduled Review: 05/28/2015
- Approval by, date: Office of Information Technology and 05/28/2014
- Revision History:
  - Supersedes (previous policy): OIT 62.8.610 Information System Recovery and Reconstitution

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard