I. Policy Statement

Cryptographic key establishment and management is necessary to reduce the risk of compromise to the measures taken for encryption of communications used by the University’s information system.

II. Purpose

This control is intended to establish the policies and procedures for the establishment and management of cryptographic keys used on the University’s information system.

III. Requirements

NSU establishes and manages cryptographic keys for required cryptography employed within the information system.

Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic key management provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.

Control Enhancements for Sensitive Systems:

1. NSU maintains availability of information in the event of the loss of cryptographic keys by users.

IV. Violations

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 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.

V. 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.