



OIT 62.805: Email Communications

Responsible Executive: Information Security Officer
Responsible Office: Office of Information Technology
Related Policy:
Approved-On Date: 2/28/2011
Effective Date: 7/1/2011
Revision Date: 2/1/2011

I. Policy Statement

The Email Communications policy reduces risks to University information by specifying control requirements that restrict access to information to only individuals who require such access as part of their job duties.

II. Purpose

Email shall not be used to send sensitive data unless encryption is used. As stated in the Encryption Policy, encryption may be required for the transmission of data that is sensitive relative to confidentiality and integrity. The ISO should consider and plan for the issue of agency email being intercepted, incorrectly addressed, or infected with a virus. An email disclaimer is a set of statements that are either pre-pended or appended to emails. These statements are frequently used to create awareness of how to treat the data in the email. An email disclaimer is not a substitute for judgment on what content to put into an email.

III. Scope

This policy applies to NSU employees and other personnel who have access to the University email system.

IV. Requirements

The University shall:

1. Require encryption for the transmission of email and attached data that is sensitive relative to confidentiality or integrity; however, digital signatures may be utilized for data that is sensitive solely relative to integrity as stated in the encryption policy. The ISO should consider and plan for the issue of agency email being intercepted, incorrectly addressed, or infected with a virus.
2. Consult with the agency's legal counsel before adopting an email disclaimer. Emails sent from University systems are public records of the Commonwealth of Virginia and must be managed as such.

The following text is an example of an email disclaimer for consideration when meeting with your agency's legal counsel.

The information in this email and any attachments may be confidential and privileged. Access to this email by anyone other than the intended addressee is unauthorized. If you are not the intended recipient (or the employee or agent responsible for delivering this information to the intended recipient) please notify the sender by reply email and immediately delete this email and any copies from your computer and/or storage system. The sender does not authorize the use, distribution, disclosure or reproduction of this email (or any part of its contents) by anyone other than the intended recipient(s).

No representation is made that this email and any attachments are free of viruses. Virus scanning is recommended and is the responsibility of the recipient.

V. 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.

VI. 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.