Policy Title: Spam Protection

Policy Type: Administrative

Policy Number: ADMINISTRATIVE POLICY # 32 – 8 – 1708 (2014) Spam Protection

Approval Date: 05/28/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

Spam protection helps to eliminate the potential for malicious or undesirable email solicitations from individuals or systems with intentions to gain information from or compromise the University’s information system.

TABLE OF CONTENTS

| Contacts                     | 1 |
| Stakeholder(s)              | 1 |
| Purpose                     | 2 |
| Requirements                | 2 |
| Violations                  | 2 |
| Interpretation              | 2 |
| Publication                 | 2 |
| 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 policy is intended to establish the policy and procedures for spam protection on the University’s information system.

REQUIREMENTS

NSU:

1. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and

2. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with University configuration management policy and procedures.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers.

VIOLATIONS

Violations of this policy will be addressed in accordance with 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 62.8.1708 Spam Protection

**RELATED DOCUMENTS**

Virginia Commonwealth State policy SEC501-08 Information Security Standard