

## UND Simple Mail Transfer Protocol (SMTP) Security Guideline

---

### Table of contents

- I. [Reason for the Guideline](#)
  - II. [Applicability of the Guideline](#)
  - III. [Guideline Statements](#)
  - IV. [Definitions](#)
  - V. [Related Documents / Policies](#)
  - VI. [Effective Dates](#)
  - VII. [Contacts](#)
- 

### I. Reason for the Guideline

E-mail is a critical service for all UND faculty, staff, and students. Our campus community depends on e-mail to communicate with one another and with the outside world. It is important to have the proper controls in place to protect the integrity and availability of this critical service. This guideline includes measures intended to prevent the spread of viruses through e-mail, to reduce spam traffic, and to promote secure access to e-mail.

### II. Applicability of the Guideline

This guideline applies to all departments or individuals who provide e-mail services using SMTP and/or connect a server using SMTP to the University of North Dakota network.

### III. Guideline Statements

All servers using the SMTP protocol should comply with the following measures prior to connection to the University of North Dakota network:

- The server using SMTP **must** be registered at [http://itsecurity.und.edu/email/server\\_registration.html](http://itsecurity.und.edu/email/server_registration.html). Only servers authorized through this process will be granted access to establish and receive port 25 connections off campus.
- All inbound and outbound e-mail messages to a server using SMTP should be scanned and cleaned of viruses, when appropriate.
- The server using SMTP should not be configured as an open relay. Also, SMTP-AUTH or similar “sender authentication” should be used whenever possible.
- All username/password (authentication) exchanges to a server using SMTP should be encrypted.

- The server using SMTP should also comply with the [NDUS Server Information Technology Security Procedures](#), when appropriate.

---

#### IV. Definitions

- Port 25      *Simple Mail Transfer Protocol (SMTP)*, documented in [Request for Comment \(RFC\) 821](#), is the Internet's standard for sending e-mail and traditionally operates over TCP, port 25. According to this UND policy, only registered and authorized e-mail servers will be allowed to send e-mail traffic off campus using port 25.
- Open relay      A server that is configured to deliver any incoming e-mail to another e-mail server without any restrictions as to whether or not the e-mail is for or from a legitimate user. Servers configured in this way are sought out by unscrupulous senders (spammers) because they give them a conduit to route large volumes of unsolicited e-mail (spam).
- SMTP-AUTH      An extension of the SMTP protocol to require a client to log in to the e-mail server during the process of sending e-mail. Servers which support SMTP-AUTH can usually be configured to require clients to use this extension, ensuring the true identity of the sender is known. SMTP-AUTH is defined in [RFC 2554](#).
- Encryption      A way of coding information so that if it is intercepted by a third party as it travels over the network, it cannot be read.

---

#### V. Related Documents / Policies

- NDUS Procedure 1901.2 Server Information Technology Security Procedures  
<http://www.ndus.nodak.edu/uploads/document-library/839/1901.2-SERVER.PDF>
- UND Port 25 Filtering Plan  
<http://itsecurity.und.edu/EmailSecurityDocuments/UND Port 25 Filtering Plan.pdf>
- RFC 821 – Simple Mail Transfer Protocol  
<http://www.ietf.org/rfc/rfc0821.txt>
- RFC 2554 – SMTP Service Extension for Authentication  
<http://www.ietf.org/rfc/rfc2554.txt>

---

#### VI. Effective Dates

Last Modified: Aug 24, 2006

Effective: Jan 22, 2007

Next Review Date: Jan 22, 2009

---

#### VII. Contacts

Contact	Phone
UND IT Security Officer (ITSO)	777-3587