CONWAY CORPORATION
OPEN MAIL RELAY POLICY

Purpose of Policy: To prohibit the use of any type of mail relaying on the Conway Corporation Network

> Corporate Mail Relay
- o Conway Corporation relaying for customers who don‘t have domains hosted with us.
  - username@domain.com

> Customer Mail Relay
- o Network users having a mis-configured mail server
- o Network users having a blatant open mail relay server

Person(s) with Responsibilities:
Will conduct technical investigations of open mail relay incidents on the Conway Corporation network as well as implement the needed technical solutions.

> Proactive Solutions:
- o As relays are discovered we will block all incoming SMTP traffic to that modem.

> Continuing notifications of the offending IP address to Conway Corporation IT staff will result in a warning to fix the problem and temporary termination of service

> Failure to comply with this will result in termination of service all together.

General Statement:
It is the policy of Conway Corporations Internet Service that no computer system managed by Conway Corporation or connected to the Conway Corporation network shall run or operate an open mail relay.

An open mail relay is a computer system that accepts and routes any email it receives without authenticating the sender. This feature was needed in the early days of the Internet to relay email from one system to another and on to its destination. However, this cooperative arrangement was eventually exploited. The email system owners soon found themselves distributing large volumes of unsolicited commercial email, known as spam, on the behalf of others and at their own expense.

Although few email servers today require open mail relay, many systems still include it as a base feature. Unfortunately, open mail relay is often activated during the install process by a novice email administrator or by a busy technician using default installation settings. Spam mailers are constantly scanning Internet for these systems and will frequently find and exploit a new open mail relay system in a matter of days.

The impact of running an open mail relay on or within the Conway Corporation have potential to cause the following consequences:

Loss of Reputation: Providing email distribution services to spammers tarnishes Conway Corporations reputation as a responsible member of Internet. The Internet Society rejects the use of open mail relay systems in their Best Current Practices documents, Request for Comments (RFC) 2505 and 2635.

Performance Degradation: Receiving, storing, and delivering large volumes of non Conway Corporation email messages places an undue strain on the resources of our email systems. Memory, disk space, CPU cycles, as well as Internet bandwidth are consumed, resulting in less than optimal performance for Conway Corporation users.

Blacklisting: In an effort to curb the spread of spam some groups, such as Mail Abuse Prevention System (MAPS), maintain a blacklist of sites that operate open mail relays. Individual site administrators frequently use these blacklists to block email originating from open mail relay sites, and in some cases will block all network traffic (i.e., web, FTP, telnet). This results in legitimate, Conway Corporation email and network traffic being blocked at the destination site.

Unnecessary Cost: The cost of processing, storage, and distribution of spam email requires more server hardware, network bandwidth, and support time than it would otherwise.

Loss of Service: The volume of spam can be great enough to render an email server inaccessible or cause it to crash.