NEBRASKA INFORMATION TECHNOLOGY COMMISSION

TECHNICAL STANDARDS AND GUIDELINES

XX-XXX Blocking Unsolicited Bulk E-Mail / "SPAM"

Category	**Groupware**
Title	**Blocking Unsolicited Bulk E-Mail / "SPAM"**
Number	**XX-XXX**

Applicability

☑ **State Government Agencies**
- ☐ All.....**Not Applicable**
- ☑ Excluding higher education institutions.....**Guideline**

☐ **State Funded Entities -** All entities receiving state funding for matters covered by this document.....**Not Applicable**

☐ **Other:** _____ .....**Not Applicable**

Definitions:
Standard - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of _____.
Guideline - Adherence is voluntary.

Status	☐ Adopted	☑ Draft	☐ Other:_____
Dates	Date: August 8, 2003 Date Adopted by NITC: Other:		

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-1506(6)
http://www.nitc.state.ne.us/standards/

1.0 Guideline

Agencies shall be allowed to evaluate and implement methods for blocking SPAM e-mail, even if some legitimate messages are blocked. Most e-mail should be accepted. Allowing the unhindered flow of legitimate state correspondence is a primary consideration of this standard. Minimum guidelines for State agencies implementing SPAM blocking methods are:

1. Must notify the e-mail originator that their message was blocked and say why.
2. Should notify e-mail originator, when possible, of alternative methods for delivering legitimate mail.
3. Should notify e-mail originator, when possible, of how to resume sending email to the state without being blocked.
4. Should not block a high volume of legitimate incoming e-mail.
5. Should not place an undue burden on Nebraska citizens for legitimate communications with the state.

2.0 Purpose and Objectives

The need for the state to access information on the Internet also allows for access from entities on the Internet into the state infrastructure, unless precautions are implemented. This guideline addresses the burden on state resources due to unsolicited bulk e-mail (UBE), spam and how state agencies may address the issue. (The term "spam" is used to denote mass unsolicited mailings, .) Agencies cannot expect to "solve" all problems that arise from bulk e-mail, only mitigate them. Policy recommendations for generally acceptable bulk e-mail practices are not addressed in this document. Agencies should use these recommendations when developing policies concerning what outside e-mail to accept.

Unsolicted email (SPAM) creates a significant drain of technical and operational resources. In 2003, the state will receive an estimated 2 million SPAM messages for approximately 12,000 employees using email. These numbers will likely continue to rise. SPAM email needs to be reduced to the extent possible without adding excessive costs or exceptional risks to normal flow of legitimate email.

2.1 Overview

The terms spam, unsolicited bulk e-mail (UBE), and unsolicited commercial e-mail (UCE) all refer to the mass posting of e-mail messages.

Any automated means of sorting out spam from e-mail messages sent by citizens, vendors, or other state agencies will result in the rejection of some valid e-mail. Agencies should take special effort to ensure that citizens can conveniently contact state agencies for official business. Blocking legitmate e-mail communication with the state should be minimized.

The goal of this guideline is not to eliminate all forms of bulk e-mail but instead to move part of the burden of dealing with unsolicited e-mail from the recipient to systems administrators. These guidelines should encourage professionalism among

e-mailers, allowing state workers to identify official correspondence more easily while not cutting off access to all bulk e-mail.

2.2 Conforming E-Mail

Most e-mail should be accepted. E-mail that conforms to the following guidelines should not be rejected without good cause. These guidelines on conforming e-mail help administrators as well as recipients to establish a chain of responsibility for the e-mail, and aid automated re-direction or deletion when appropriate. Non-conformance to these guidelines does not imply the agency must necessarily reject the message, but senders who repeatedly send non-conforming e-mail are recognized as unnecessarily adding to the administrative burden of the state's e-mail systems. In general, state agencies should accept bulk e-mail that meets the following minimum requirements.

(1) The sender is identifiable and can be contacted by e-mail. The e-mail contains a valid e-mail address for the sender of the message. If the originator of the message is not the same as the person or company actually sending the message, valid e-mail contact information for both is present.
Valid return addresses allow state workers to respond to e-mail directly, if appropriate, without resorting to the phone, postal mail, or any other method that may be unavailable or inconvenient. Phone numbers and/or postal addresses may be included in addition to the e-mail reply addresses.

(2) The sender discloses how the means of obtaining the e-mail address. The message contains a statement on how the sender obtained the recipient's e-mail address. State agencies and their workers have an interest in how the e-mailer obtained the e-mail address, and this is a vital part of the "chain of responsibility" required of bulk e-mailers. Details of how the addressee got on the list can be given by including lines such as the following within the body of the e-mail message: "This e-mail list was derived from your attendance at the Fall COMDEX conference."

(3) The recipient must "OPT-IN" before being sent any repeat mailings. If the e-mailing was unsolicited, then this must be a one-time-only mailing. A recipient who does not want to receive addition mailings on a topic must not be forced to perform any action. Any repeat mailings can only be as the result of an explicit action on the part of the recipient, such as a request for additional information or to be added to a list.

(4) The sender identifies the e-mail address the message was sent to. Whether for a single mailing or for an opt-in list, the sender must include within the body of the message a statement identifying the full e-mail address the message is being sent to, such as: This message was sent out to: joe.smith@state.ne.us This inclusion allows users and administrators to keep track of e-mail that might pass through multiple computers, aliases, or internal agency e-mail lists before reaching the final recipient, and to help identify e-mail being sent to persons no longer employed by the agency or no longer working in the same capacity.

(5) The recipient is informed how to be removed from the mailing list. The recipient must be informed how to be removed from the mailing list within the body of the message. Just because a recipient doesn't want to be on a particular list does not imply they want to refuse all unsolicited e-mail. The remove instructions must distinguish between being removed from the current list, and all lists maintained by the sender. Merely directing the recipient to a general "list of people who don't want to be on lists" is not sufficient to comply with this guideline.

(6) The message is "reasonably targeted" to the addressee. An unsolicited e-mail should only be sent to someone who might reasonably, in high percentage, be interested in reading the message. See the definitions of "targeted", "narrowed", and "indiscriminate" e-mail lists, below.

2.3 Examples of E-Mail That Should Be Rejected

(1) E-mail that cannot be traced to a valid source computer. When the apparent originating computer of an e-mail has no name, or an invalid name, such as when that computer's name does not appear in the Domain Name System (DNS) database of computer names, that e-mail may be rejected. As with any other rejection criteria, e-mail senders with legitimate state business may be denied access because their computer is merely miss-configured, or because of some temporary outage within the DNS database. Invalid source addresses, however, are the mainstay of senders who don't wish to be properly identified, and this is one area where many illegitimate senders can be eliminated.

(2) E-mail relayed without permission. E-mail that was relayed without permission through another computer in an effort to disguise its origin or to place the burden and expense of e-mail delivery upon another computer may be rejected out of hand.

(3) E-mail from addresses or domains posted on the state's subscribed black list. E-mail that is received from sources that have a history of delivering spam. This list of sources are provided to the state through a subscribed service.

2.4 Methods for Blocking SPAM

SPAM Blocking techniques have costs, effectiveness, and usage issues to consider. Agencies may investigate and use the following methods:

DNS Reverse Name Look-up - Blocks SPAM from the most troublesome SPAM producers. This method is easy to implement but has the greatest risk of blocking legitimate email. IT is very difficult for Email senders to understand or fix problems.

White list - Blocks almost all SPAM, but is difficult to implement and confusing for external email senders to understand. Many Email senders will refuse to add their ID to a state white list.

Blacklist - Likely to block 60% of SPAM but is likely to block a small percentage of legitimate email. It is fairly easy to implement, email senders are notified the mail was blocked, and many know what a blacklist is.
Router Blocking - Looks at a manually prepared list of site domain names or IP addresses to block. This method only blocks specific email known to be a problem. This method may not impact the worst SPAM producers. It is easy to implement, but is manually intensive to maintain. Users may not understand the cryptic message sent by a router.
Filtering - May block a significant number of SPAM Messages at a fairly low cost. Some legitimate messages may be blocked. It is fairly easy to implement. Users will see a customized message from most systems. One type of filtering is "Content Filtering". It involves searching for text in body, subject, or the sender information. Another type of filtering is "Blocking", which is based on the number of addresses in the recipients field. It can also use the file extension name or the size of memo.
Personal Rules - User creates rule to delete from in-box. The cost is high, because each individual has to learn how to set up rules. Usually, rules are not very effective against the worst SPAM producers.

2.5 Other Resources

The Internet Mail Consortium (IMC) has published several reports on the problem. "Unsolicited Bulk Email: Mechanisms for Control" (http://www.imc.org/ube-sol.html) lists the technical and legal solutions being discussed and how they affect Internet mail users. "Unsolicited Bulk Email: Definitions and Problems" (http://www.imc.org/ube-def.html) provides precise definitions of UBE and spam issues.

The Coalition Against Unsolicited Commercial Email (http://www.cauce.org/) is also a source of information.

3.0 Definitions

3.1 Targeted e-mail list

A "targeted" e-mail list is a collection of e-mail addresses where the sender may reasonably expect that all or nearly all of the addressees will be interested in the solicitation. An example of this would be a list of conference attendees, where the conference host may reasonably assume that past attendees will be interested in notification about future, similar conferences. Targeted lists are generally acceptable.

3.2 Narrowed e-mail list

A "narrowed" e-mail list is a collection of addresses that can be expected to contain a higher-than-average percentage of addressees interested in the solicitation. An example of this would be the use of a list of computer conference attendees to send a solicitation for the purchase of computer cabling services. While such conference attendees may be more likely than the general population to have an interest in such a solicitation, such a broad solicitation might be an unreasonable transfer of costs from the sender to the recipient when only a small percentage of the total recipients

are likely to be interested, even though that percentage is higher than would be found on an indiscriminate list.

3.3 Indiscriminate e-mail list

An "indiscriminate" list is one where the sender would have little or no reasonable expectation that the addressee would have more interest in the solicitation than the general population. An example of this would be the sending of a notification of "investment opportunities" to e-mail addresses culled randomly from posters to Usenet newsgroups. "UBE/Spam" e-mail is identified most often with indiscriminate e-mail. The sending of solicitations to state workers as part of a indiscriminate e-mail list is almost always unacceptable.

4.0 Responsibility

Information Management Services Division may investigate and implement methods for the mail routing server, which IMServices supports. Other agencies may elect to share this service or set up their own.

5.0 Related Policies, Standards and Guidelines

Nebraska Information Technology Commission, Individual Use Policy:
http://www.nitc.state.ne.us/tp/workgroups/security/policies/individual_use_policy.pdf

State of Nebraska Acceptable Use Policy of State Data Communications Network,
http://www.doc.state.ne.us/policies/datausage.html