NEBRASKA INFORMATION
TECHNOLOGY COMMISSION

# TECHNICAL STANDARDS AND GUIDELINES

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

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

| | |
|---|---|
| Applicability | ☑ **State Government Agencies,** excluding _______________ .................... **Standard**<br>☐ **State Government Agencies,** all .......**Not Applicable**<br>☐ **State Funded Entities -** All entities receiving state funding for matters covered by this document.................**Not Applicable**<br>☐ **Other:** ____________ .........................**Not Applicable**<br><br>**Definitions:**<br>**Standard** - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of ______________.<br>**Guideline** - Adherence is voluntary. |

| | |
|---|---|
| Status | ☐ Adopted ☑ Draft ☐ Other:_________ |
| Dates | Date: June 30, 2003<br>Date Adopted by NITC:<br>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 Technical Standard

Agencies must develop and implement procedures to control what outside e-mail to accept and when to send bulk e-mail to employees, business partners and associates, constituents, and clients. Most e-mail should be accepted. Allowing the unhindered flow of legitimate state correspondence is a primary consideration of this standard. All state agencies must:

A. Publish a clear set of policies about what is acceptable and unacceptable use of e-mail services.
B. Incorporate e-mail policies as part of their on-line privacy policy notice. In particular, agencies that provide on-line registration for events, newsletters, or other services must explain how e-mail address may be used by the agency and if e-mail addresses will be shared with third parties.
C. Comply with guidelines in this document for distributing bulk e-mail.
D. Insure adequate technical support for maintaining e-mail services for controlling the following unsolicited bulk e-mail (UBE) / SPAM issues:
   1. Restrict e-mail UBE / SPAM at the mail transport agent;
   2. Restrict Usenet UBE / SPAM at the news server;
   3. Restrict known UBE / SPAM sites at the network router;
   4. Stop outgoing UBE / SPAM by not relaying unauthorized e-mail.
E. (Incident reporting requirement?)

## 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 (The term "spam" is used to denote mass unsolicited mailings, see RFC2635), and how state agencies may address the issue. 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 addressed. Agencies should use these recommendations when developing policies concerning what outside e-mail to accept, as well as their own practices when sending outgoing bulk e-mail to employees, constituents, and clients.

### 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. In some cases "bulk e-mail" can be anticipated notices from professional organizations, selected publications and routine communications from vendors to their customers or from government agencies to citizens. The different categories of e-mail are difficult to distinguish from each other, and any attempt to block one type of e-mail category can result in the unintended blocking of some e-mail that should have gone through.

Spam and UBE messages often offer get-rich-quick schemes, or commercial solicitations for goods and services that are not desired by the recipient. By analogy, with US Postal codes for paper based junk mail, and laws addressing unsolicited FAX transmissions, agencies have the right to reject e-mail delivery to their workers for whatever reasons they deem appropriate, and most UBE/spam mail should be ignored. Yet any automated means of sorting out this type of e-mail from e-mail messages sent by citizens, vendors, or other state agencies will result in the rejection of some valid e-mail. Agencies should, therefore, tread lightly in this area, and take special effort to ensure that citizens can conveniently contact state agencies for official business. Citizens attempting to send e-mail to a state agency may already be frustrated by attempts to contact the agency through some other means, and blocking their ability to communicate with the state should be minimized.

With judicious filtering an agency can be reasonably certain that they will not be rejecting a high percentage of e-mail that should have been accepted, but the percentage will never be zero. Allowing the unhindered flow of legitimate state correspondence is a primary consideration in this guideline.

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 off of the recipient. 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 Background

State of Nebraska Acceptable Use Policy of State Data Communications Network, http://www.doc.state.ne.us/policies/datausage.html, addresses issues for agencies to consider in establishing policy for what is permissible for state employees to distribute electronically and what is not. However, the sending of unsolicited bulk e-mail (UBE) or spam through a state agency system or network can occur from external sources if agency servers allow e-mail relay by unauthorized users.

Unsolicited Bulk E-Mail or spam sent through state agency systems or networks could be illegal in Nebraska. See Nebraska Penal Code, Sections 28-1341 to 28-1348, Computer Crimes Act. This law makes it illegal to "access" meaning "to ... instruct, communicate with, store data in, ... or otherwise make use of" any resource of a computer, computer system, or computer network without the effective consent of the owner. "Information resources residing in the various agencies of state government are strategic and vital assets belonging to the people of Nebraska. These assets must be available and protected commensurate with the value of the assets."

State agencies need to establish policies for employee use, the majority of work to prevent unauthorized use will fall on network and e-mail system administrators. Internet mail administrators will have to balance the needs of authorized users and provide reliable services for local and remote access.

## 2.3 Conforming E-Mail

Most e-mail should be accepted. E-mail that conforms to the following guidelines should not be rejected without extraordinary 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 e-mail systems. In general, state agencies should accept bulk e-mail that meets the following minimum requirements. State agencies should follow these same guidelines for all of their own outgoing bulk e-mail:

**(1) A sender who 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 must disclose how they obtained 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) A 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 must identify 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 must be 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.

## 2.4 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.

## 2.5 Other Considerations

Not all state agencies may have systems administrators who know all aspects of Internet communication. It takes training and time to become qualified to perform many of these e-mail filtering solutions. Regardless of vendor claims, don't expect to install a commercial product and get the desired results if your system administrator does not have a thorough understanding of Internet e-mail and DNS protocols.

### 2.6 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.