**Montana Judicial Branch**

**Administrative Policies**

|  |  |
| --- | --- |
| **Subject: Electronic Mail** | **Policy No.: 1530** |
| **Chapter:** | **Number of Pages: 2** |
| **Section: Computer Usage** | **Revision Date: June 17, 2017; April 5, 2022** |
| **Effective Date: July 1, 2002** |  |

# Policy

This policy applies to all Judicial Branch employees, contractors, and local government employees using a state-owned computer.

The state-provided electronic mail (e-mail) system is to be used for: the conduct of state and local government business and delivery of government services; transmitting and sharing of information among governmental, research, and educational organizations; supporting open research and education in and between national and international research and instructional institutions; communicating and exchanging professional information; encouraging debate of issues in a specific field of expertise; applying for or administering grants or contracts; announcing requests for proposals and bids; announcing new services for use in research or instruction; and conducting other appropriate state business.

Judicial Branch employees are required to use the state provided e-mail system for state business purposes unless they do not have direct connection to SummitNet, the state’s internal network. Qualifying use of an external e-mail system must be approved by the Judicial Branch IT Security Officer and SITSD.

All messages created, sent, or retrieved over the state's systems are the property of the State of Montana. Privacy of e-mail is not guaranteed; employees should not have the expectation of Privacy for any messages. It is the expectation that any message sent is subject to public scrutiny. Employees should never send any messages with Personally Identifying Information (PII) or Protected Health Information (PHI) over the e-mail system. The use of encryption should be considered when sending these types of messages, or use of an alternative method to send documents such as the state’s file transfer service, or MT Drive.

Stationery may be used when it enhances the business content of e-mail. Stationery, moving graphics and/or audio objects should not be used unnecessarily since they consume more resources, such as disk space and network bandwidth, and tend to detract from the message content.

SITSD reserves the right to block e-mail from specified domains, from specific e-mail addresses, or e-mail that contains specific information in the subject line. These filters may be put into place because of the effect on the state’s e-mail system or computer network.

E-mail on personal mobile devices is permissible if the employee’s job function necessitates. Connectivity to e-mail services must be done in accordance with the state’s Mobile Device Policy and follow all procedures within that policy. Access to state e-mail cannot be provided if a personal device is not compliant with state policy.

Any e-mail received that is unsolicited or suspicious in nature should not be opened and should be reported to the security officer for investigation.

# Misuse of E-Mail

The following items represent, but do not constitute either an exhaustive or exclusive listing of, misuse of state e-mail resources:

## Circulating chain letters.

## Using the state e-mail system for: 1) “for-profit” activities, 2) “non-profit” or public, professional or service organization activities that aren't related to an employee’s job duties, 3) extensive use for private, recreational, or personal activities, or 4) political activity.

## Sending messages with Personal Identifiable Information (PII) or Protected Health Information (PHI) in an unsecured manner.

## Statewide distributions of e-mail. The Supreme Court Information Technology Division should be contacted for correct procedures for large e-mail distributions.

## Using personal e-mail accounts for state business.

# Guidelines and Recommendations

Employees should check e-mail with a frequency appropriate to the job duties. If employees are unable to check e-mail for an extended period of time, they should use the “auto reply” feature in Outlook or make arrangements to have the mail received by someone else and reviewed in an appropriate time frame.

The chance of receiving a virus or malware increases with the use of e-mail. Many forms of malware come embedded in attachments. Suspicious e-mail messages should be forwarded to the security office for investigation and not opened.

Employees should strive to keep e-mail message and attachment size as small as possible. All attachments over one megabyte (1MB) should be compressed (zipped) prior to sending. Employees are encouraged to use archive folders to maintain e-mail in compliance with records retention policies.

In drafting e-mail and sending e-mail messages, employees are reminded that they should not include anything they are not prepared for the public to read. E-mail communications should resemble typical professional and respectful business correspondence.

# Retention of E-mail:

E-mail retention will be in compliance with the standards adopted through the Judicial Branch Records Retention policy and will be archived and retained as directed. Official correspondence related to fiscal, human resources, procurement, or other administrative matters shall be retained with the original subject materials. For instance, e-mail correspondence about a procurement issue will be maintained in the procurement file; individual retention of these e-mails is not required. E-mails printed and maintained in a paper file should not be maintained electronically.

E-mails produced as part of routine ministerial functions such as scheduling meetings, exchanging information about basic office procedures, and unsolicited sales contacts should be deleted.

When an official or employee terminates employment, the assigned supervisor shall follow the process established by information technology to capture and retain the contents of the e-mail as required in the retention policy.

# Compliance

Failure to comply with any or all the portions of this policy is grounds for disciplinary action up to and including termination.

# References and Authorities

2-17-533; 2-17-534, MCA

# Closing

## Level of training required: (A) All court officials and employees. (1) Read only.

## Questions concerning this policy should be directed to the Information Technology Director or IT Security Officer, Office of the Court Administrator, Montana Supreme Court.