HR/LR Policy #1423

Appropriate Use of Electronic Communication and Information Technology

Date Issued: 11/15/1997
Date Revised: 10/16/2002, 6/26/2006, 1/3/2012, 12/7/2021, 12/11/2023, 07/01/2024
Authority: MMB Enterprise Employee Resources and Minnesota IT Services

OVERVIEW

Objective

Establish standards for the acceptable use of the state's information technology (IT) resources and define the appropriate use of electronic communication.

Policy Statement

The purpose of the state's IT resources is to further the business of the state. Personal use of state IT resources is permitted only as provided in this policy.

Employees who violate this policy may be subject to discipline, up to and including discharge. Violation of this policy also may subject individuals to criminal penalties as provided in M.S. 43A.39 and other law.

Scope

This policy applies to all employees of executive branch agencies (M.S. 43A.02, subds. 2 & 22) and includes all employees of the Minnesota State Retirement System, Public Employees Retirement Association, and Teachers Retirement Association.

Definitions and Key Terms

Key Term	Definition
Incidental Use	Personal use of state IT resources that is minimal in terms of duration and frequency.
Incremental Cost	A cost, loss of time, or loss of resources that is so small as to make accounting for it unreasonable or administratively impracticable.
Information Technology (IT) Resources	Software, hardware (e.g., computers, telephones, etc.), documentation, programs (e.g., email, voicemail, etc.), systems, networks, information, equipment, and devices owned, leased, or provided by the state.

Statutory References

M.S. 43A.38, subd. 4 Code of Ethics for Employees in the Executive Branch, Use of State Property
M.S. Ch. 13 Government Data Practices
M.S. 138.17 Government Records; Administration
5 U.S.C. 7321-7326 Hatch Act
18 U.S.C. 119 Wire and Electronic Communications Interception
18 U.S.C. 2701-2711 Stored Wire and Electronic Communications and Transactional Records Access

GENERAL STANDARDS AND EXPECTATIONS

This policy should be read in conjunction with other applicable policies, including Minnesota Management and Budget (MMB) HR/LR policies, procedures and general memos, and Minnesota IT (MNIT) Enterprise Information Security Policies and Standards.

Employees who violate this policy may be subject to discipline, up to and including discharge. Violation of this policy also may subject individuals to criminal penalties as provided in M.S. 43A.39 and other law.

I. Reasonable Use

Personal use of state IT resources is permitted only if the use, including the value of the time spent:

(1) Does not increase risk to state data or system security
(2) Results in no more than an incremental cost to the state
(3) Complies with state and federal law, this policy, and applicable enterprise security, MMB, and agency-specific policies

Employees' personal use of state IT resources must be occasional, incidental use only, and must be limited to break and lunch time whenever possible. More than occasional, incidental use of state IT resources, including during nonwork time, is not permitted. Any personal use of state IT resources must not interfere with an employee's job duties.

Employees are expected to use good judgment when using state IT resources, whether for personal or state business purposes. All state business-related electronic communications and all use of state IT resources must be able to withstand public scrutiny without embarrassment to the agency or the State of Minnesota, and must be appropriate in type, tone, and content. Employees are responsible for the content of their state and personal use of state IT resources and may be subject to discipline up to and including discharge, criminal penalties, or liability resulting from that use.

II. Prohibited Use

The following use of state IT resources is **always prohibited**, even if it is incidental or includes no cost for the state:

- Activities that violate state or federal law
- Activities that violate M.S. 43A.38 or HR/LR Policy #1445 Code of Ethical Conduct
- Activities that violate any MMB, MNIT, or agency policies, including but not limited to, anti-discrimination and anti-harassment policies and procedures, HR/LR Policy #1432 Respectful Workplace, HR/LR Policy #1329 Sexual Harassment Prohibited, HR/LR Policy #1436 Harassment and Discrimination Prohibited, and HR/LR Policy #1444 Workplace Violence
- Wagering, betting, or selling
- Speaking on behalf of, or giving the impression of speaking on behalf of, the state or any agency without authorization, including but not limited to using the employee's state email address for non-work-related communications
- Conducting commercial or nonprofit business activities except on behalf of the state
- Engaging in non-state outside employment
- Performing personal work (e.g., finances, investments, purchases, legal correspondence, class note-taking or homework except for classes approved by the supervisor as work-related)

- Using any state video conferencing technology (including Teams, etc.) for non-work related purposes unless all parties attending are state agency employees
- Sending emails containing not public government data to the employee's personal email, unless the email contains not public data only about the employee
- Sending emails or other electronic messaging containing not public government data through unsecured email or Internet systems unless the data are encrypted
- Shopping, game playing, or streaming entertainment unless required by the employee's job responsibilities or otherwise authorized by the agency
- Performing work for non-work related organizations (e.g., social, political, religious)
- Political activities prohibited by M.S. 43A.32 Political Activities, M.S. 211B.09 Prohibited Public Employee Activities; Administrative Procedure 32 Political Activities of State Employees; the federal Hatch Act; or other applicable state or federal laws
- Campaigning for partisan or non-partisan elected or appointed office of a public or private entity
- Fundraising or soliciting for any purpose unless expressly authorized by the agency
- Allowing access or use by any person who is not a state agency employee (e.g., family members or friends)
- Accessing state IT resources with another employee's credentials (e.g., username or password), or providing one's own credentials to others to access state IT resources
- Sending chain letters
- Unauthorized accessing of data that is not public
- Unauthorized transportation of state data or systems to or access from any location outside the United States, without prior approval, as per MNIT's International Travel Policy
- Using state IT resources in a manner that creates the impression that the state or any agency endorses or prefers any religion or religious practice
- Viewing, storing, downloading, transmitting, or soliciting violent, obscene, sexually explicit, or pornographic materials, unless required by the employee's job responsibilities
- Storing or transferring government data to any other systems or platforms that have not been approved by MNIT
- Using any software or other state IT resources in a manner or access not according to the applicable software license agreement

III. Protection Against Malicious Electronic Communications

Use of electronic communications for business purposes increases the chances that state agency employees will be exposed to malicious electronic communications. These malicious communications could be in many forms: email, text message, web site, phone call, or even video meeting. Employees are expected to react in a manner consistent with protecting state information and resources.

React Appropriately

If a suspected malicious electronic communication is received, do not react in a manner dictated by the communication. Do not click links in the email or text message. Do not click a button on an unexpected pop-up that appeared when visiting the web site. Any communications about the suspected communication should be outside of the channel in which it was received. For example, if an email is suspicious, call the individual listed as the sender using a known telephone number.

Report Suspicious Communications

All suspicious electronic communications must be reported to the Security Operations Center.

IV. Use of Email for Union Activity

Employees may use their state email address and state email systems to communicate with their exclusive representatives regarding the following activities so long as the use does not increase risk to state data or system security, results in no more than incremental cost to the state, and is otherwise consistent with this policy and other applicable policies and law:

- Collective bargaining
- The administration of collective bargaining agreements
- The investigation of grievances and other workplace-related complaints and issues
- Internal matters involving the governance or business of the union

Other than communication with exclusive representatives regarding matters related to the employee's job, such activity must occur outside of employees' work hours, except as provided by collective bargaining agreement.

V. State email addresses and the state email system may not be used in violation of the federal Hatch Act, including but not limited to political activities or fundraising Monitoring Activities

Monitoring Activities

State IT resources are state property. The state (including any state agency and MNIT) may, in its sole discretion and for any lawful purpose, monitor, inspect, access, read, examine, copy, delete, seize, use, share, disclose, confiscate, or take any other action with respect to state IT resources. The state may also take such action with respect to any and all data collected, created, sent, received, accessed, maintained, processed, or stored by state IT resources, at any time and for any lawful purpose. The state is not required to provide notice to users. Additionally, telephone and Internet voice calls may be monitored or recorded. Any monitoring or recording of telephone calls will comply with state and federal law.

Access/Disclosure and Use

Any and all data related to the Monitoring Activities described in this section may be accessed by or disclosed to state agency employees whose job assignments reasonably require access, MNIT Services, Minnesota Management and Budget, civil or criminal enforcement authorities, and any other person or entity authorized by state or federal law or court order, and may be used in civil or criminal proceedings, disciplinary proceedings, employment, civil or criminal investigations, audits, or for any other lawful purpose.

Consent and No Expectation of Privacy

Use of state IT resources constitutes consent to the Monitoring Activities, Access/Disclosure, and Use described in this section. There is no expectation of privacy in state IT resources, or in the use of state IT resources, even when the use is for personal purposes. The state maintains the right to conduct Monitoring Activities for personal use of state IT resources to the same extent that it has the right to conduct Monitoring Activities with respect to use for state purposes, and personal use is subject to Access/Disclosure and Use as described in this section to the same extent as use for state purposes.

RESPONSIBILITIES

Agency Responsibilities

- Adopting and enforcing the provisions of this policy
- Developing supplemental addenda as needed to address agency-specific needs regarding the appropriate use of the state's (IT) resources that are consistent with this policy and the law

MMB Responsibilities

- Administration and maintenance of this policy in conjunction with Minnesota IT Services

Employee Responsibilities

- Comply with all provisions of this policy
- Report suspicious electronic communications appropriately
- Comply with MNIT Services' security measures and standards
- Comply with agency-specific policies and procedures

FORMS AND INSTRUCTIONS

The Acknowledgement Form for HR/LR Policy #1423 Appropriate Use of Electronic Communication and Information Technology is included in annual ELM training for all state agency employees.

REFERENCES

HR/LR Policies

1429 Data Protection for Human Resource Systems
1432 Respectful Workplace
1329 Sexual Harassment Prohibited
1436 Harassment and Discrimination Prohibited
1444 Workplace Violence Prohibited
1445 Code of Ethical Conduct
1438 Mobile Device Use

Administrative Procedures

32 Political Activities of State Employees

Enterprise Information Security Policies & Standards: Security

CONTACTS

MMB Human Resource Management and Labor Relations

Minnesota IT Services