Internet Acceptable Use

Number: ENT-INT-011

Established for: State of Montana Information Technology Enterprise

BARBARA RANF, Director
Department of Administration
August 2, 2001

SCOPE

This policy applies to all state employees and state contractors using a state computer. This policy does not apply to public access computers, and students/employees of the Montana University Systems who are employed by the System and are not full time employees.

INTERNET ACCEPTABLE USE

The State provided Internet, intranet and related services are 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.

The State provided Internet, intranet and related services are not to be used 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, or 3) for extensive use for private, recreational, or personal activities.

Employees should not have expectations of privacy for Internet use. Agency System Administrators, management, and Department of Administration personnel can monitor Internet usage for planning and managing network resources, performance, troubleshooting purposes, or if abuses are suspected.

Employees must follow all other state policies when using the state provided Internet service. See policy ENT-SEC-081 User Responsibilities for additional information regarding the use of state computer resources.

COPYRIGHT LAWS

State employees must honor copyright laws regarding protected commercial software or intellectual property. Duplicating, transmitting, or using software or other electronic property not in compliance with license agreements is considered copyright infringement. State employees are not to make copies of any copyrighted materials without the full legal right to do so. Unauthorized use of copyrighted materials or another person's original writings is considered copyright infringement. Copyrighted materials belonging to others may not be transmitted by staff members on the Internet without permission. Users may download copyrighted material from the Internet, but its use must be strictly within the agreement as posted by the author or current copyright law. In addition, copyrighted agency/State information used on web sites must be clearly labeled as such.

AGENCY RESPONSIBILITIES RELATED TO THE INTERNET

Each agency must have a clear policy on their business use of the Internet, intranet and related services. The policy should detail the permissible and non-permissible uses of the Internet, intranet and related services for their agency business use.

Background - History on the creation of or changes to this policy

The ITAC Internet Policy Advisory Task Force worked during 1997 to study the need for policy for state government use of the Internet. The Task Force identified potential areas of risk, researched existing policy and law, and determined whether there was additional need for policy. The Task Force found that educating agencies and employees with a compilation of existing policy, law and guidelines would provide direction to agency and employee Internet users. The results of the Task Force's work are this policy and its guidelines and recommendations to ITAC regarding changes to existing policies.

The ITAC Internet Policy Advisory Task Force was comprised of representatives from the following agencies and organizations:

The Commissioner of Higher Education, the Public Service Commission, the Department of Agriculture, the Department of Administration's Information Services Division, the Department of Commerce, the Department of Transportation, the Department of Environmental Quality, the Department of Justice, the Office of Public Instruction, the Legislative Branch, the Department of Public Health and Human Services, the State Fund, the State Auditor's%2, 0Office, the State Library, the Governor's Office, the Department of Fish, Wildlife and Parks, the Department of Labor and Industry and the Department of Revenue

Guidelines - Recommendations, not requirements

The Internet has been provided to State employees for the benefit of agencies and their customers. Every State employee has the responsibility to maintain and enhance the State's

public image and to use the Internet in a productive manner. To ensure these standards are being met, the following guidelines have been established for assisting agencies in developing their agency business use policies for the Internet, intranet and related services.

"Don't say, do, write, view, or acquire anything that you wouldn't be proud to have everyone in the world learn about if the electronic records are laid bare."

Agencies should be in compliance with existing statewide and agency laws, rules and policies. Following are some examples of the existing laws, rules and policies for consideration when creating agency business use policies. Other laws, rules and policies may be applicable.

LAWS AND RULES

- MCA 2-2-121 - Rules of Conduct for Public Officers and Public Employees
- MCA 2-17-533 - Electronic Access Systems
- MCA 45-6-311 - Unlawful Use of a Computer
- ARM 2-21-1105 - Cost/Benefit Analysis Criteria
- ARM 2.13.101 - 2.13.107 - Regulation of Communication Facilities
- MOM 1-0250.00 - Information System Security
- MOM 1-0232.30 - Central Software Support Services
- MOM 1-1103.01 - Use of State Telephone System, Personal Telephone Use

*In addition, agencies should be aware that issues of Federal law and individual rights may also apply.

POLICIES

- SummitNet Acceptable Use
- Aggressive Use of Information Technology to Provide Citizen Access to Information and State Services
- Transmission Privacy
- Computer Virus Detection & Prevention
- User Responsibility
- Network and File Server Security

Each agency must have a clear policy on their business use of the Internet, intranet and related services. The policy should detail the permissible and non-permissible uses of the Internet, intranet and related services for their agency business use. Following are items and examples for consideration when creating agency business use policies. Other issues may be applicable.

User Responsibility

Number: ENT-SEC-081

Established for: State of Montana Information Technology Enterprise

BARBARA RANF, Director
Department of Administration
August 2, 2001

Policy - Requirements

SCOPE

This policy applies to all state employees and state contractors using a state computer. This policy does not apply to students/employees of the Montana University Systems who are employed by the System and are not full time employees.

REQUIREMENTS

Each user of the State of Montana's computing and information resources should realize the fundamental importance of information resources and is responsible for the safe keeping of these resources.

Users and system administrators must guard against abuses that disrupt or threaten the viability of all systems, including those on the State network and those on networks to which State systems are connected.

Each user is responsible for having knowledge of the State's policies concerning security and care for their computer. It is the responsibility of the State to educate its management and staff about these policies; to educate its employees about the dangers of computer abuse and its threat to the operation of the State computer network; and educate its management and staff about proper ethical behavior, acceptable computing practices, and copyright and licensing issues.

Each user of the State of Montana's computing and information resources must act responsibly. Each user is responsible for the integrity of these resources. All users of State-owned or State-leased computing systems must be knowledgeable of and adhere to agency policies, respect the rights of other users by minimizing unnecessary network traffic that might interfere with the ability of others to make effective use of this shared network resource, respect the integrity of the physical facilities and controls, and obey all federal, state, county, and local laws and ordinances. All employees must abide by these policies, relevant laws and contractual obligations, and appropriate ethical standards.

State computing facilities and UserIDs are to be used for the job-related activities for which they are assigned. State computing resources are not to be used for the following:

- private commercial purposes,
- non-State-related activities (including games or software that is not required for an employees job responsibilities), or
- non-State standard software. Exceptions can be granted by ITSD for the use of software for which a State standard exists.

MISUSE OF COMPUTER RESOURCES

The following items represent, but do not fully define, misuse of computing and information resources:

- Using computer resources to create, access, download, or disperse derogatory, racially offensive, sexually offensive, harassing, threatening, or discriminatory materials.
- Down-loading, installing, or running security programs or utilities which reveal weaknesses in the security of the state's computer resources unless a job specifically requires it.
- Use of computers and UserIDs for which there is no authorization, or use of UserIDs for purpose(s) outside of those for which they have been issued.
- Attempting to modify, install, or remove computer equipment, software, or peripherals without proper authorization. This includes installing any non-work related software on State-owned equipment.
- Accessing computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer, software, data, information, or network in question is owned by the State. (That is, if you abuse the networks to which the State has access or the computers at other sites connected to those networks, the State will treat this matter as an abuse of your computing privileges.)
- Circumventing or attempting to circumvent normal resource limits, logon procedures, and security regulations.
- The use of computing facilities, UserIDs, or computer data for purposes other than those for which they were intended or authorized.
- Sending fraudulent e-mail, breaking into another user's e-mailbox, or unauthorized personnel reading someone else's e-mail without his or her permission.
- Sending any fraudulent electronic transmission, including but not limited to fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions or journal vouchers, or fraudulent electronic authorization of purchase requisitions or journal vouchers.

- Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization.
- Taking advantage of another user's naivete or negligence to gain access to any UserID, data, software, or file that is not your own and for which you have not received explicit authorization to access.
- Physically interfering with other users' access to the State's computing facilities.
- Encroaching on or disrupting others' use of the State's shared network resources by creating unnecessary network traffic (for example, playing games or sending excessive messages); wasting computer time, connect time, disk space, or other resources; modifying system facilities, operating systems, or disk partitions without authorization; attempting to crash or tie up a State computer; damaging or vandalizing State computing facilities, equipment, software, or computer files).
- Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner.
- Reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission.
- Knowingly transferring or allowing to be transferred to, from or within the agency, textual or graphical material commonly considered to be child pornography or obscene as defined in 45-8-201(2), MCA.

REPORTING AND DISCIPLINARY ACTION

Users will cooperate with system administrator requests for information about computing activities; follow agency procedures and guidelines in handling diskettes and external files in order to maintain a secure, virus-free computing environment; follow agency procedures and guidelines for backing up data and making sure that critical data is saved to an appropriate location; and honor the Acceptable Use Policies of any non-State networks accessed.

Users will report unacceptable use and other security violations to their immediate supervisor, to local personnel responsible for local network policy enforcement, or to personnel responsible for the security and enforcement of network policies where the violation originated.

Misuse of the state's computer resources may result in an agency taking disciplinary action appropriate to the misuse, up to and including termination.