Montana Judicial Branch

Administrative Policies

|  |  |
| --- | --- |
| **Subject: Acceptable Computer Use** | **Policy No.: 1510** |
| **Chapter:** | **Number of Pages: 4** |
| **Section: Computer Usage** | **Revision Date: June 6, 2017** |
| **Effective Date: July 1, 2002** |  |

# Policy

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

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 individually responsible for knowing the Judicial Branch’s policies concerning security and care for their computer. It is the responsibility of the Judicial Branch to educate its management, staff and users 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 to educate its management, staff and users about proper ethical behavior, acceptable computing practices, copyright, and licensing issues. **There is no expectation of privacy while using the State’s IT resources.** All activity can be logged, monitored and reviewed. Devices must be locked when leaving them unattended, except when in a controlled area. Users must log off of devices at the end of the day unless permission has been received to run a job or process. All work related files and electronic information shall be stored on the states network to ensure the document(s) are backed up. Users shall report missing or stolen IT hardware immediately to their supervisor and to the Judicial Help Desk. They shall also notify the Judicial Help Desk in the event of a security incident, or if the device is acting unusual, e.g. slow performance, or unexpected popup advertisements are occurring. If remote access is required, it must be requested by the user’s supervisor, and approved by the appropriate Judicial Branch information technology staff, and must utilize state approved software.

Each user of the state’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 know and adhere to applicable 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 comply with 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 User IDs are to be used for job-related activities for which they are assigned. State computing resources are not to be used for the following:

## Private, commercial, or political purposes.

## Non-state-related activities. This policy does not prohibit the reasonable use of electronic mail for private, recreational, or personal activities implicitly authorized by the separate policy on electronic mail.

## Nonstandard software is not to be installed without the explicit permission of the Judicial Branch information technology staff.

# Misuse of Computer Resources

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

## 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

## Use of unapproved cloud-based services for data storage, transfer, etc. is prohibited.

## User must never share User ID’s or passwords.

## Users shall not plug-in *non-State* owned storage media (USB storage devices, external or internal hard drives), including *personal* mobile devices (iPads, Kindles, smartphones, etc.) to the workstation or internal network.

## Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner.

## 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.

## Using computer resources to create, access, download, or disperse derogatory, racially offensive, sexually offensive, harassing, threatening, or discriminatory materials.

## Downloading, 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 User IDs for which there is no authorization, or use of User IDs 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 Information Technology Services Division and the Supreme Court Information Technology Division will treat this matter as an abuse of your computing privileges.)

## Circumventing or attempting to circumvent normal resource limits, logon procedures and security regulations.

## Employees must never attempt to gain access to, disclose, or remove any user ID, information, software, or file that is not their own and for which they have not received explicit authorization to access.

## 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 naiveté or negligence to gain access to any User ID 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 computer games, streaming non work related video, or sending excessive messages); wasting disk space (for example, storing pictures, music, or files that are personal) 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).

## 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.

# Violations

Actual or suspected violations of this policy must be reported to the Supreme Court Information Technology Help-Desk at 1-800-284-6017.

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

# References and Authorities

2-17-534; 2-15-114; 45-6-311; 2-2-121, MCA; MOM.

# Closing

## Level of training required: (A) All court 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.