USER INFORMATION SYSTEM USAGE POLICY

I. General Statement – The Unified Judicial System (UJS) serves the people of Alabama through thousands of employees located in offices and courthouses throughout the State. The UJS is called upon to deliver more efficient services to a growing population that rightfully expects ever-increasing improvements in service. By utilizing modern information technology such as computers, the internet, and e-mail, the UJS can serve the citizens of Alabama more efficiently.

Taxpayers have the right to depend on their government to manage their tax dollars wisely and effectively. Public confidence in the productiveness of government is increased when members of the public are confident that their government is well managed and assets are used appropriately. UJS employees are expected to follow rules and regulations and to be responsible for their own personal and professional conduct. By following these mandatory guidelines and policies, UJS employees and users of UJS computer equipment and services can assure that their actions are responsible.

The UJS recognizes employees and officials as responsible individuals who are the key to making government more responsive to its citizens. These policies and guidelines establish additional responsibilities for UJS employees and officials when utilizing such technology. They allow employees to use government office equipment for non-governmental purposes when such use involves minimal additional expense to the government, is performed on the employee's non-work time, does not interfere with the mission or operations of a department or agency and does not violate the State ethics laws, other law, or other personnel policies and guidelines. The guidelines and policies below also inform JS employees and users of UJS computer equipment and services that any expectation of privacy is waived by using any such equipment or services.

II. Scope

These policies and guidelines apply to all UJS officials, employees, and individuals and organizations conducting business for and on behalf of the UJS and Administrative Office of Courts (AOC) through contractual relationships when using JS resources. They also apply to all individuals utilizing UJS computer equipment, internet services, and e-mail systems. The policies and guidelines apply to teleworking, travel and other off-site locations as well as all of the office locations of the UJS. They do not supersede any other applicable law or higher level agency directive or policy guidance. UJS department heads and office managers shall apply these policies and guidelines not just to UJS employees, but also to contractor personnel, interns, and other non-government individuals through incorporation by reference in contracts or memorandums of agreement as conditions for using UJS provided resources.

III. Purpose

The purpose of these policies and guidelines is to:

- Ensure UJS employees and other individuals utilizing UJS computer equipment, internet services, and e-mail system are informed about the applicability of policies, guidelines, and laws.
- Ensure users are aware of what UJS deems as acceptable and unacceptable use of its computer equipment, internet services, and e-mail system.
- Ensure computer, internet, and e-mail services are used in compliance with those policies, guidelines, and laws.
- Specify potential sanctions that may be imposed as a result of a user's failure to follow the policies and guidelines set forth herein.
- Specify how instances of misuse will be investigated and prosecuted where applicable.
- Specify that UJS employees and users of UJS computer equipment, internet services, and e-mail systems cannot have a reasonable expectation of privacy with regard to electronic communications or activity.

A. UJS Information Systems are in place to facilitate your ability to perform your job efficiently and productively. These systems are solely for that purpose. Only "incidental personal use" as stated in this policy, which does not interfere with work or use Alabama resources, shall be allowed.

B. The AOC may intercept and monitor communications on its Information Systems for purposes including, but not limited to, penetration testing, communications security, network operations, network defense, personnel misconduct, and law enforcement investigations.

C. At anytime, the AOC may access, inspect, and seize data stored, relayed, or transmitted on its Information Systems. Communications using or data stored on AOC systems are not private are subject to monitoring, interception, access, search, and may be disclosed or used for any authorized purposes.

D. The AOC purchases and licenses the use of various computer software programs for official purposes. Unless authorized by the software developer, the AOC does not have the right to reproduce such software for use on more than one computer. Employees may only use software on Information Systems according to the software license agreement. Illegal duplication of software and its related documentation for personal use is also prohibited.

E. The downloading or installation of freeware or shareware is prohibited. These programs often hide malicious code and create an unacceptable security risk. All software installations shall be done by the IT department and only after a risk has been determined to be non-existent by the IT Section and approved by the IT Director of the AOC.

F. E-mail is provided by the AOC to enhance communications. Employees shall ensure that information contained within email messages and other transmissions is legal, accurate, appropriate, and ethical. Jokes, chain letters, spam, etc., take up valuable bandwidth, slow down system resources, and allow the easy spread of viruses, worms, and Trojan horses.

G. Internet access is provided by the AOC to grant access to information required for official use. Employees shall not use AOC Information Systems for personal financial gain (except to monitor retirement plans). Prohibited activities include but are not limited to, commercial activities, purchasing of personal items, pornographic sites, gaming sites, auction sites and gambling sites.

H. Copyright, Patent, and Trademark information shall be identified and marked as required by law.

I. Passwords are unique to each individual and are critical for access controls and user authentication. It is strictly prohibited for individuals to divulge their passwords to anyone to include supervisors and IT personnel. Furthermore, users are prohibited from obtaining or attempting to obtain another individual's password or logon credentials. Users shall notify IT Security if someone has or suspects someone has attempted to logon with their credentials. Users shall also contact the IT Helpdesk to have their password reset if it is compromised.

J. Blog and chat sites pose a high security risk, as well as an operational security risk. Therefore, all chat and blog sites are prohibited on AOC Information Systems. Exceptions to this policy are professional blog and chat sites that have had a security risk assessment accomplished by IT Security and approved by the IT Director of the AOC.

K. Portable Devices offer mobility and greater flexibility than standard systems; however, they also present unique security issues. All AOC owned portable devices shall have usernames/passwords established for access controls and authentication purposes. The systems shall have a screen saver/lockout feature that activates after five minutes of inactivity. Also, all data storage drives shall use approved encryption protocols. Users shall report lost or stolen portable devices to the IT Department immediately. Furthermore, employees shall obtain supervisor permission prior to removing any data or information system devices from AOC facilities. All data and devices shall be inventoried prior to removal.

L. Devices that are not purchased or owned by the AOC or the UJS are prohibited and shall not be connected to the UJS network. Devices include, but are not limited to, hubs, switches, portable hard drives, thumb drives, notebooks, Palm Pilots, etc. Any non-UJS device that is found attached to UJS Information Systems shall be confiscated by the IT Department. The item shall be held and not returned to the user until a security threat analysis is completed by IT Security and approved by the IT Director.

M. Confidential Documents include personal medical data, personal protected information, privileged court documents, etc. These documents are protected under privacy laws and are not to be released to the public. When documents are emailed outside of the UJS network, the AOC is still legally liable; however, the State cannot guarantee proper protection mechanisms. Therefore, confidential documents shall not be emailed outside of the UJS Information Systems (to include home) without authorization from the IT Director.

N. Users shall not tamper, alter, or attempt to alter any Information System configuration setting, device, or security mechanism. This includes, but is not limited to, attempting to bypass password/logon systems, screen saver lockout devices, editing or deleting of audit logs, interfering with or disabling of encryption devices/software, etc.

O. As indicated in this policy, Information Systems, email, and Internet access are reserved for work related activities. Occasional personal use is permitted within the following guidelines: Emailing short messages to family members and friends, personal banking needs, retirement accounts (RSA, 401, etc), and browsing of news and weather sites are acceptable personal use activities.

P. Personnel requiring specific exceptions to this policy may request a waiver from the IT Director in writing. The waiver request should include the specific paragraph(s) that the waiver is intended, the justification for the waiver, and the duration of the requested waiver. The IT Director shall approve or disapprove each waiver request on a case by case basis.

Q. The IT Department recognizes that occasionally Judges, District Attorneys, probation officers, etc., may require access to prohibited sites for investigations and research for on-going cases. For IT needs to support on-going investigations, contact the IT Director.

R. Your consent to and compliance with these Information System policies is a term and condition of use of UJS Information Systems. Failure to abide by these policies or failure to consent to any interception, monitoring, copying, reviewing, and downloading of any communications or files is grounds for removal from the UJS network as a user.

IV. Distribution of Policy - This policy will be communicated and issued to all Administrative Office of Courts officials, administrators, managers, and employees.

V. Federal, State and Local Laws – Where this policy differs from federal, state or local laws, this policy will conform to those laws as the AOC's Legal Department may advise.

VI. Review and Revision – The AOC reserves the right to rescind and/or amend this policy and all Organization policies at any time.

AOC Access Information Form – Municipal Courts

To Be Completed by the Approved Authorized Individual on Record with AOC

Name:	
Login/User Name (ex. Jane.Doe):	
SSN (Last 4 Digits):	
Site Address:	
City, State, Zip Code:	
Municipal Court of:	
Phone Number	
User's Job Title:	
User's Immediate Supervisor:	

Please Select the User Type:

- ☐ Municipal Chief Magistrate
- ☐ Municipal Court Clerk
- ☐ Municipal Judge
- ☐ Municipal Magistrate
- ☐ City Prosecutor
- ☐ Other _____

Type of Access Requested:

- ☐ New Access
- ☐ Update Access
- ☐ Remove Access

Enter Existing AC# _____

User Is: ☐ Contractor ☐ Volunteer ☐ Auditor **eMail Address**: _____

SJIS Level of Access: **(Indicate the Level of Access for EACH of the Following Categories)**

☐ **No SJIS Access Changes**

Confidential
- ☐ None
- ☐ Look Only
- ☐ Add / Change
- ☐ Delete

Index
- ☐ None
- ☐ Look Only
- ☐ Add / Change
- ☐ Delete

Traffic
- ☐ None
- ☐ Look Only
- ☐ Add / Change
- ☐ Delete

Payments / Accounting
- ☐ None
- ☐ Look Only
- ☐ Add / Change
- ☐ Delete

Youthful Offender
- ☐ None
- ☐ Look Only
- ☐ Add / Change
- ☐ Delete

Witness / Party
- ☐ None
- ☐ Look Only
- ☐ Add / Change
- ☐ Delete

Municipal Criminal
- ☐ None
- ☐ Look Only
- ☐ Add / Change
- ☐ Delete

Online Case Action Summary
- ☐ None
- ☐ Look Only
- ☐ Add / Change

Warrants
- ☐ None
- ☐ Look Only
- ☐ Add / Change
- ☐ Delete

Citation History
- ☐ None
- ☐ Look Only

Case MGR Screen
- ☐ None
- ☐ Look Only
- ☐ Add / Change
- ☐ Delete

District Criminal
- ☐ None
- ☐ Look Only
- ☐ Add / Change
- ☐ Delete

Grand Jury
- ☐ None
- ☐ Look Only
- ☐ Add / Change
- ☐ Delete

Other Access:

AOC Email:
- ☐ **YES**
- ☐ **NO**

AlacourtPlus:
- ☐ **MY CLERK**
- ☐ **MY JUDGE**
- ☐ **AlaVault Only**

AlaVault Access Levels:

Public Folder:
- ☐ **Search Only**
- ☐ **Scan**
- ☐ **Edit / Delete**

Private Folder:
- ☐ **Search Only**
- ☐ **Scan**
- ☐ **Edit / Delete**

eCitations (eSwear & eSearch)
- ☐ **YES**
- ☐ **NO**

Municipal Court Annual Report Portal:
- ☐ **YES** **Public IP Address:** _____
- ☐ **NO**

Office / Bank Accounts
☐1 ☐2 ☐3 ☐4 ☐5
☐6 ☐7 ☐8 ☐9

_____
Signature, Authorizing Officer Date

_____
Signature, User Date

I acknowledge receipt of the User Information System Usage Policy and will abide by its guidelines as part of my access to the Administrative Office of Court's Network and associated electronic applications.

All AOC Access Forms for MUNICIPAL COURTS should be eMailed to: Municipal Support at AOC. Please eMail a completed, signed form to MunicipalSupport@alacourt.gov. If you have any questions regarding this form, please email us or call us at: 1-866-954-9411 Option 1, Option 6 or 334-954-5006. * **Please see attached Privacy Act Statement.**

Privacy Act Statement

AUTHORITY	Executive Order 10540.50 U.S.C.781, et seq. DLA Privacy Act System Notice S 500.50, Access & Badging Records, applies.
PRINCIPAL PURPOSE(S)	Personal information on this form is used to grant the individual access to a sensitive DLA Automated Information System (AIS). The provided information is used to ensure that only authorized personnel have access to this system.
ROUTINE USE(S)	Information from this system may be disclosed for any of the DLA blanket routine uses.
DISCLOSURE	Disclosure of information on this form is voluntary. However, if the information is not provided , system access will be denied.