ADMINISTRATIVE OFFICE OF COURTS

Virtual Private Network (VPN)

1. Overview

Virtual Private Network (VPN) technologies are an extension of a private network that enable remote users to access UJS applications and networked resources over a dedicated private link. Though encrypted, VPN tunnels are not infallible, and AOC assumes risks when individuals connect with VPN technology.

2. Purpose

The purpose of this policy is to establish policy and guidelines for remote access to UJS Information Systems via VPN connections and technologies.

3. Scope

This policy applies to all individuals who utilize VPN technology to access UJS data, applications, or network resources that reside on UJS Information Systems to include on-prem and cloud services.

4. User Requirements

a) Individuals granted VPN privileges are responsible to ensure that their VPN accounts are protected, and any other users or individuals do not use said account. Passwords are unique to each individual and are critical for access controls and user authentication.

b) It is strictly prohibited for individuals to divulge their passwords to anyone, to include supervisors. Furthermore, it is prohibited for individuals to obtain or attempt to obtain another individual's passwords or logon credentials. Users shall notify IT Security if someone has or suspects someone has attempted to logon with their credentials.

c) By utilizing VPN technology, users consent that the machine are a de facto extension of the UJS network, and as such, are subject to the same rules and regulations that apply to the UJS network.

d) By utilizing VPN technology, users consent that their actions may be monitored by AOC and that they do not have an expectation of privacy.

e) Pings, trace routes, and other network mapping actions are not authorized while utilizing the VPN unless specifically authorized by the IT Director.

f) Users shall not bypass or attempt to bypass any security protocol while utilizing the VPN.

5. Technology Requirements

a. VPN gateways and accounts shall be managed and maintained by the IT Security Department.

b. All VPN traffic and connections are subject to monitoring. 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. Users shall be disconnected after 30 minutes of inactivity.

d. Computers shall meet all security protocols and will be enforced by the firewall. Users of systems that do not meet minimal security requirements shall be given instructions on how to correct the deficiency. Systems shall be disconnected from the VPN until all security protocols are met.

e. Split-tunneling is on a case-by-case basis and shall be done by URL exception. Blanket split-tunneling is prohibited.

6. Enforcement

a. Your consent to and compliance with these VPN policies is a term and condition of use of the VPN technology.

b. Enforcement shall be through technical and policy implementations. Users that fail to abide by these policies or failure to consent to any interception or monitoring of any communications shall have their VPN account disabled and VPN privileges revoked.

State of Alabama Unified Judicial System Form IT-01 Rev. 10/24	**VPN ACCOUNT REQUEST**	

Date:_____ **Phone Number:**_____

Last Name:_____ **County:**_____

First Name:_____ **Office/Org:**_____

User Name:_____ **Job Title:**_____

E-Mail:_____ ☐ **New** ☐ **Change** ☐ **Remove**

State Property Tag #: _____ **Operating System:** _____

Make/model #: _____

Justification:

By signing this form, I state that I have read and shall comply with all requirements and guidelines contained within the AOC VPN Policy letter.

_____ Date:_____

Signature

Internal Use Only

Approved By:	**Created By:**	**Date:**