ACCEPTABLE USE POLICY

Prepared by
TECHNOLOGY SERVICES DIVISION | INFORMATION SECURITY OFFICE
June 2025 | v. 3.14

TABLE OF CONTENTS

About the North Carolina Judicial Branch
The mission of the North Carolina Judicial Branch is to protect and preserve the rights and liberties of all the people as guaranteed by the constitutions and laws of the United States and North Carolina by providing a fair, independent, and accessible forum for the just, timely, and economical resolution of their legal affairs.

About the North Carolina Administrative Office of the Courts
The mission of the North Carolina Administrative Office of the Courts is to provide services to help North Carolina's unified court system operate more efficiently and effectively, considering each courthouse's diverse needs, caseloads, and available resources.

1 Purpose

The purpose of this **NCAOC Acceptable Use Policy** ("AUP") is to outline the acceptable rules of behavior for Organizational Users who access and use Information Technology Resources provided by the North Carolina Administrative Office of the Courts (NCAOC) in compliance with the **NCAOC Planning Policy** and **NCAOC Planning Procedures**.

This policy will:

- establish the minimum, acceptable rules of behavior with which Organizational Users must comply regarding access to and use of Information Technology Resources;
- comply with applicable federal and state law and other rules and regulations;
- establish Organizational Users' obligation to acknowledge they understand and agree to the acceptable use and access requirements in this policy; and
- strive to protect Information Technology Resources from unauthorized access, use, disclosure, or transmission and from misuse, loss, Vulnerability, compromise, and a Security Breach.

2 Audience

The audience for this policy includes all Organizational Users who access or use Information Technology Resources, and who are responsible for managing Information Technology Resources, information technology, and the NCAOC Information Security, Risk, Assurance, and Privacy Programs.

3 Scope

This policy and any associated procedures, guidelines, or plans function within the overall framework of NCAOC policies, procedures, guidelines, and plans established in support of NCAOC Information Security, Risk, Assurance, and Privacy Programs, as authorized by the NCAOC Chief Technology Officer.

Exceptions to this policy must be based on an assessment of any associated Risk, any compensating or mitigating controls, and the written acceptance of that Risk.

This policy applies to Organizational Users' access and use of Information Technology Resources. This policy supersedes the **NCAOC Electronic Messaging, Internet and Computer System Use Policy** adopted in April 2012. When applicable, Organizational Users should include security planning controls in contracts or agreements with Third Parties.

This policy satisfies G.S. § 143-805(c), which requires that the Judicial Branch adopt a policy governing the use of NCAOC Networks and Devices owned, leased, maintained, or otherwise controlled by the Judicial Branch.

While this policy does not apply to Non-Organizational Users, all Users who elect to access the Guest Wireless Network using a non-NCAOC-issued, personal device shall acknowledge the terms of the Guest Wireless Disclaimer prior to connecting to the Guest Wireless Network.

4 Definitions

For Definitions, see the **Glossary** located on Juno at:
https://juno.nccourts.org/resources/references/glossary-acceptable-use-and-generative-ai-policies.

5 Roles and Responsibilities

5.1 NCAOC Director

The NCAOC Director approves this policy and monitors the application of this policy in coordination with the Chief Technology Officer.

5.2 Chief Technology Officer (CTO)

On authority delegated by the NCAOC Director as the authorizing official for NCAOC Information Systems, the NCAOC CTO monitors the application of this policy in coordination with the NCAOC Director and the NCAOC Chief Information Security Officer.

5.3 Chief Information Security Officer (CISO)

The NCAOC CISO coordinates the development, documentation, and dissemination of this policy working in collaboration with the NCAOC CTO, NCAOC Risk Management Officer, and NCAOC Privacy Officer to oversee implementation and enforcement of this policy.

5.4 Risk Management Officer

The NCAOC Risk Management Officer reviews this policy in coordination with the NCAOC CISO and NCAOC Privacy Officer.

5.5 Privacy Officer

The NCAOC Privacy Officer reviews this policy, ensuring this policy considers and addresses any privacy Risks.

5.6 Technology Services Division

The NCAOC Technology Services Division (TSD) is responsible for providing Information Technology Resources to Organizational Users for use, granting access to Information Technology Resources, and providing NCAOC Information System and System Component administration, including monitoring Organizational Users' computer policy compliance and investigating and Remediating privacy- or security-related Events. TSD reserves the right to request the return of, limit the use of, or disable access to Information Technology Resources for Organizational Users who violate this policy.

5.7 Human Resources Division

The Human Resources Division works in coordination with the NCAOC Director, CTO, CISO, and Office of General Counsel to investigate, evaluate, advise, and when necessary, recommend appropriate disciplinary action for, violations of this policy.

5.8 Judicial Branch Officials and Hiring Authorities

All Judicial Branch Officials and Hiring Authorities shall ensure that Organizational Users reporting to them remain in compliance with this policy.

5.9 Organizational Users

Organizational Users are responsible for using Information Technology Resources as outlined in this policy.

6 Policy Statement

6.1 Use of Technology

a. This policy describes what Organizational Users can do and not do when using Information Technology Resources. This policy also outlines actions the NCAOC may take to perform Judicial Branch business and protect Information Technology Resources, other Judicial Branch assets, and Organizational Users.

b. By using Information Technology Resources, Organizational Users agree to comply with this policy and applicable state or federal laws.

c. This policy applies to:
   1. Organizational Users who access or use Information Technology Resources provided by the NCAOC;
   2. authorized Collaborative Computing applications and devices that are connected to the Judicial Branch Network and use NCAOC Internet addresses; and
   3. actions originating from computer systems or mobile devices maintained or used by Organizational Users connecting remotely to the Judicial Branch Network or Websites bearing the NCAOC or Judicial Branch credentials, even when hosted outside the NCAOC's Internet domain.

d. General usage of Information Technology Resources is permitted for Organizational Users within the limitations set forth in this policy.

e. For privacy and security purposes, all Organizational Users shall connect all **NCAOC-issued** devices only to the Judicial Branch Network – not the Guest Wireless Network.

f. Organizational Users may access a Judicial Branch Cloud Application on premises or remotely as follows:
   1. When using an NCAOC-issued device using the Judicial Branch On-Premises Network or Judicial Branch Wireless Network, Organizational Users can access a Judicial Branch Cloud Application to access, store, process, or create Data.
   2. When using an NCAOC-issued device to access a Judicial Branch Cloud Application remotely on a home or other private network (e.g., hotel, coffee shop, airport, etc.), Organizational Users are **required** to use their NCAOC-supported Virtual Private Network (VPN). If NCAOC-supported VPN or other remote access options are not viable, Organizational Users may also use NCAOC-supported Virtual Desktop Infrastructure (VDI), if such VDI use has been approved by the CTO.
   3. When using a non-NCAOC-issued device, Organizational Users are allowed to use Judicial Branch Cloud Applications remotely, if authentication and authorization have been granted by the NCAOC.

Remainder of Page Intentionally Left Blank

Table 1

Device Type	Judicial Branch On-Premises Network	Judicial Branch Wireless Network	Guest Wireless Network	Home and Other Private Network (e.g., hotel, coffee shop, airport, etc.)
NCAOC-Issued Device	Organizational Users are **required** to use **NCAOC-issued devices** when connected to the Judicial Branch On-Premises Network. Active Directory authentication and authorization is required. Multi-factor authentication (MFA) is required if the Organizational User has not been prompted for MFA over the last fourteen (14) days.	Organizational Users are **required** to use **NCAOC-issued devices** when connected to the Judicial Branch Wireless Network. Active Directory authentication and authorization is required. MFA is required if the Organizational User has not been prompted for MFA over the last fourteen (14) days.	Organizational Users are **prohibited** from using **NCAOC-issued devices** on the Guest Wireless Network. No MFA is required.	When using an **NCAOC-issued device**, Organizational Users are **required** to use their NCAOC-supported VPN when connected to a home or other private network (wired or wireless). If NCAOC-supported VPN or other supported remote access options are not viable, Organizational Users may also use NCAOC-supported VDI, if such VDI use has been approved by the CTO. Active Directory authentication and authorization is required. MFA is required for VPN.
Non-NCAOC - Issued Device	Organizational Users are **prohibited** from **connecting non-NCAOC-issued devices** to the Judicial Branch On-Premises Network. Cisco Identity Services Engine (ISE) is used to prohibit non-AOC devices from being used on the Judicial Branch Network from a wired perspective.	Organization Users are **prohibited** from connecting **non-NCAOC-issued devices** to the Judicial Branch Wireless Network. MFA is not applicable.	Organizational Users are **allowed** to use **non-NCAOC-issued devices** on the Guest Wireless Network. MFA is not applicable.	When using a **non-NCAOC-issued device**, Organizational Users are **allowed** to use a home and other private network (wired or wireless) to use Judicial Branch Cloud Applications remotely, **if authentication and authorization have been granted by the NCAOC.** MFA is required.

6.2 Personal Use of Technology

a. Organizational Users are provided the use of Information Technology Resources to perform Judicial Branch business functions and deliver services.

b. Organizational Users shall adhere to the limitations in **Table 1** above regarding accessing, storing, processing, or creating Data when using non-NCAOC-issued, personal devices (e.g., laptops, tablets, cellular telephones).

c. The use of Information Technology Resources and services should be consistent with Judicial Branch and Hiring Authority goals, provide services to North Carolina citizens, enable innovative and cost-effective ways to improve services, and promote professional growth.

d. Organizational Users' "reasonable personal use" of Information Technology Resources during personal, non-work hours is allowed; however, personal use shall be kept to a minimum during the Organizational Users' work hours and shall not cause NCAOC Information System performance degradation, impact the privacy or security of NCAOC Information Systems, the Judicial Branch Network, or services, or have a negative impact on Organizational Users' work performance or productivity. **Reasonable personal use does not include supporting or opposing political campaigns.** Additionally, all activity (including limited personal use) using Information Technology Resources or services, must adhere to all Judicial Branch policies. The NCAOC reserves the right to curtail usage of the Judicial Branch Network, Guest Wireless Network, and NCAOC Information Systems.

6.3 Inappropriate Content

a. While the Internet and social media platforms may contain legitimate business and personal content, they also include content that is inappropriate for Organizational Users to access. Inappropriate content includes without limitation, content containing nudity, violence, illegal drugs, sexually explicit content, pornography, obscenity, and gambling. Inappropriate content shall not be accessed, stored, or utilized by Organizational Users while at work, or while using Information Technology Resources. Organizational Users must use common sense and consideration for others in deciding which content is appropriate for the workplace.

b. Judicial Branch leadership understands that specific Organizational Users in certain job roles may require some exceptions to **Section 6.3.a** as they have a legitimate business need to access, store, and utilize content of an "inappropriate" nature as part of their job functions. In the event the Organizational User needs to access inappropriate content as part of their job functions, the Hiring Authority of the Organizational User shall submit an Unblock Site Request ticket to the NCAOC Help Desk. Approval of an Unblock Site Request shall be deemed an exception to **Section 6.3.a** of this policy.

c. **Section 6.4.b.** below governs requests by Judicial Branch elected officials or employees to view Pornography in the course of that elected official's or employee's official duties. The Judicial Branch elected official or employee must be engaged in one or more of the activities listed below in **Section 6.4.a.1. through 7.**

d. The NCAOC Branch employs technical controls to monitor this policy (see **Section 6.7**, **Technical Controls** below.).

6.4. Prohibition on Viewing or Storing Pornography on Judicial Branch Networks and Devices

In addition to complying with the inappropriate content restrictions outlined above in **Section 6.3**, North Carolina has issued a new law, effective October 1, 2024, mandating that the Judicial Branch shall: (1) "not permit the viewing of pornography by its employees on a network of the judicial branch" (G.S. § 143-805(a)); (2) "not permit an employee, elected official, or appointee of the judicial branch to view pornography on a device owned, leased, maintained, or otherwise controlled by the judicial branch" (G.S. § 143-805(b)); and (3) adopt a policy governing the use of its networks and devices, including disciplinary actions for violations no later than January 1, 2025 (G.S. § 143-805(c)). The following provisions implement these statutory requirements:

a. Judicial Branch **employees, elected officials, or appointees** shall not view or store Pornography on Judicial Branch Networks or on a Device owned, leased, maintained, or otherwise controlled by the Judicial Branch **unless** that Judicial Branch **employee, elected official, or appointee** is engaged in any of the following activities in the course of their official duties listed in G.S. § 143-805(d):
    1. Investigating or prosecuting crimes, offering or participating in law enforcement training or performing actions related to other law enforcement purposes;
    2. Identifying potential security or cybersecurity Threats;
    3. Protecting human life;
    4. Establishing, testing, and maintaining firewalls, protocols, and otherwise implementing G.S. § 143-805;
    5. Participating in judicial or quasi-judicial proceedings;
    6. Conducting or participating in an externally funded research project at one of the constituent institutions of The University of North Carolina; or
    7. Researching issues related to the drafting or analysis of the laws of the State of North Carolina as necessary to fulfill the requirements of the employee's official duties as an employee of the Judicial Branch.

b. In the event a Judicial Branch elected official, appointee, or employee is engaged in any of the activities as outlined above in **Section 6.4.a.1. through 7.**, the elected official, appointee, or the Hiring Authority of the employee shall submit an Unblock Site Request ticket to the NCAOC Help Desk. Approval of an Unblock Site Request shall be deemed an exception to **Section 6.4.a** of this policy.

c. Judicial Branch **employees**, **elected officials,** and **appointees** who have Pornography saved to any Device owned, leased, maintained, or otherwise controlled by the Judicial Branch must remove, delete, or uninstall that Pornography **no later than January 1, 2025**, **unless** the Judicial Branch **employee, elected official,** or **appointee** is, in the course of their official duties, engaged in any of the activities listed above in **Section 6.4.a.1. through 7.** and has submitted their Unblock Site Request in compliance with **Section 6.4.b**.

d. Disciplinary action for violations of **Section 6.4** is governed by **Section 10** of this policy. (G.S. § 143-805(c))

6.5 Additional Prohibitions on Unacceptable Use

a. The actions included herein shall also constitute **unacceptable use** of Judicial Branch Applications, the Judicial Branch Network, or a Third-Party Network. This list is not exhaustive. It is included to provide a frame of reference for the types of activities that are deemed unacceptable.

b. Organizational Users shall not use Information Technology Resources to:
    1. Engage in an activity that is illegal under local, state, federal, international, or other applicable laws, including U.S. copyright law, or that fails to comply with Judicial Branch policies.
    2. Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the Judicial Branch.
    3. Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, threatening, harassing, bullying, obscene or otherwise inappropriate messages or media.
    4. Engage in activities that cause an Invasion of Privacy.
    5. Engage in activities that cause disruption to the workplace environment or create a hostile workplace environment.
    6. Make fraudulent offers for products or services.
    7. Perform any of the following: port scanning, security scanning, network sniffing, or keystroke logging.
    8. Perform cyberattacks or other IT Data gathering techniques when not part of the Users' specific job functions.
    9. Pirate software.
    10. Illegally obtain copyrighted works or other materials, which may include, but are not limited to, music, streaming services, movies, games, etc.
    11. Reveal Judicial Branch user IDs or passwords to others, including Users, family, friends, or other members of the Organizational Users' household.
    12. Render unreadable or block authorized access to any Data, document, or electronic file using non-NCAOC-issued encryption software.
    13. View or stream audio or video in an excessive manner that is not required to perform Judicial Branch business.
    14. Participate in online games.
    15. Access or attempt to access computer systems using Information Technology Resources, including those external to the NCAOC, without authorization by the owner of that system.
    16. Send electronic communication messages or create Web pages with fraudulent address or header information or containing misrepresentations in authorship or content in an attempt to deceive others.
    17. Use Information Technology Resources in a way that would constitute a regular private business activity.
    18. Deliberately misuse trademarks in Web pages and email, including Judicial-owned trademarks, such as the official logo or seal and trademarks owned by other entities.
    19. Provide false or misleading information in order to obtain access to Information Technology Resources.
    20. Use any device or software which degrades the performance of Information Technology Resources.
    21. Damage or attempt to damage Information Technology Resources.
    22. Deliberately or recklessly introduce computer Viruses, Worms, or other types of Malware technologies which would harm the Integrity of Information Technology Resources as well as attempt to create or disseminate such technologies.
    23. Deliberately or recklessly misuse Information Technology Resources which interfere with the ability of other Organizational Users to access or use NCAOC Information Systems or the Judicial Branch Network or degrade the performance of NCAOC Information Systems or the Judicial Branch Network, including techniques to disguise or obscure the source of Data network traffic.

24. Send unsolicited bulk electronic communication (spam) unrelated to the Judicial Branch's mission or related bulk email without appropriate prior approval.

6.6 Malware and Data Loss Prevention

a. The online criminal community utilizes both general Web and social media sites to deliver Malware and carry out schemes designed to damage property or steal Confidential Data. To minimize Risks related to such Threats, adhere to the guidelines listed below. While these guidelines help to reduce Risk, they do not cover all possible Threats and are not a substitute for good judgment.
   1. Do not use any NCAOC-provided email addresses to create credentials (i.e., user IDs and/or passwords) for personal activities (e.g., social media, e-Commerce (shopping), or registration on non-business-related sites). NCAOC-provided email addresses may be used for work related activities, such as official Judicial Branch business, participation in professional organizations, and continuing education. Threat actors can potentially compromise NCAOC Information Systems when Organizational Users use their NCAOC-provided email address and/or password(s) as their credentials for other systems.
   2. Do not use the **same** passwords for Websites that you use to access Information Technology Resources.
   3. Do not follow links or download software from individuals or organizations that you do not know. NCAOC Information Systems are provisioned with the necessary software for most Judicial Branch operational needs. If there is additional software needed, Organizational Users are required to contact the NCAOC Helpdesk for guidance and assistance in advance of installation to ensure they do not put Information Technology Resources at Risk.
   4. Do not install any File Sharing software on NCAOC-issued devices without written approval from the NCAOC Information Security Office.
   5. Do not use or insert non-NCAOC-issued Digital Media (i.e., flash drives, jump drives, thumb drives, etc.) into NCAOC-issued devices.
   6. When on NCAOC-issued devices, if any Websites or social media content looks suspicious in any way, close your browser and do not return to that page.

6.7 Technical Controls

a. This policy is monitored and enforced by TSD. Technical controls are in place on NCAOC Information Systems and the Judicial Branch Network to monitor inbound and outbound Judicial Branch Network communications to assist in enforcement of this policy and prevent internet-based attacks (Malware, phishing, etc.).

b. To ensure security controls remain updated to protect against the latest cybersecurity Threats, and to also ensure NCAOC Information System Vulnerabilities are addressed in a timely fashion, Organizational Users are required to connect any NCAOC-issued Information Technology Resources such as laptops to the Judicial Branch Network weekly. Remote connection via NCAOC-supported VPN meets this requirement. In addition, when NCAOC-supported VDI is provided because NCAOC-supported VPN or other remote access options are not viable, NCAOC-supported VDI also meets this requirement, so long as such VDI use has been approved by the CTO.

c. Organizational Users' failure to connect their NCAOC-issued Information Technology Resources to the Judicial Branch Network at least weekly for one (1) hour may result in those Information Technology Resources being temporarily disconnected from the Judicial Branch Network and NCAOC-issued services until all necessary updates are applied.

d. TSD reserves the right to block Organizational Users' access to internet sites that may degrade Judicial Branch Network performance; send traffic into or receive traffic from outside the United States; or have little or no business purpose (e.g., streaming movie sites, online games, cloud sharing sites, etc.).

6.8 No Expectation of Privacy

a. Organizational Users should understand that when using the Judicial Branch Network or other Information Technology Resources, there is no implicit or explicit expectation of privacy. Such use may include the Handling of files, Data, and messages.

b. Subject to state and federal laws, attorney-client privilege, and judicial privilege, the NCAOC reserves the right to monitor, review, log, report, copy, inspect, or retrieve all use of the Judicial Branch Network or Information Technology Resources. The NCAOC also has the right to disclose such unauthorized use of Information Technology Resources to authorized recipients, including law enforcement.

Note: Having no expectation of privacy does not in any way waive the Judicial Branch's right to protect its non-public, Confidential Data or waive attorney-client privilege or judicial privilege.

6.9 Custody of Data

a. Organizational Users have a responsibility to ensure the Confidentiality, Integrity, and Availability of Data. Organizational Users are strongly encouraged not to store Confidential Data on their personal devices since they do not own this sensitive Data. They should also refrain from storing any personal information (photographs, correspondence, videos, etc.) on Information Technology Resources.

b. Also, there are various NCAOC employees and independently-elected court officials whose constitutional or statutory authorities include maintaining the custody of Data stored on Information Technology Resources. As a custodian of the Data, these Organizational Users may have other specific responsibilities.

6.10 Bandwidth Usage

Network Bandwidth is not an unlimited resource. Networks are essential to conducting business for the Judicial Branch. Excessive consumption of network bandwidth will be monitored and adjusted to provide priority for business-related functions.

6.11 Circumvention of Security

Organizational Users are prohibited from using Information Technology Resources to circumvent any security systems, authentication systems, User-based systems, or from escalating access privileges without prior authorization and approval (e.g., sharing passwords or user IDs, not using MFA, not informing NCAOC about improper levels of access when assuming a new role). Tampering with NCAOC security controls or taking any actions to bypass or circumvent the privacy and security of Information Technology Resources is expressly prohibited.

6.12 Protecting Confidential Data

a. Organizational Users must take all reasonable efforts to protect PII and other non-public, Confidential Data.

b. PII is incorporated by reference into the public records law pursuant to G.S. § 132-1.10(b)(5). PII and other Confidential Data in the **NCAOC Data Classification Policy** must be encrypted At Rest and in transit or as otherwise determined by the NCAOC CISO to be adequately protected (e.g., stored in a drive specially secured by the NCAOC).

c. Please note that electronic records may be requested in bulk unless "individually available online in a format that allows a person to view the public record and print or save the public record to obtain a copy" or available under a contract with the NCAOC for remote public access. G.S. §§ 7A-109(d) and 132-6.1(a1); *LexisNexis Risk Data Mgmt. v. N.C. Admin. Office of the Courts*, 368 N.C. 180, 775 S.E.2d 651 (2015). In the event of a public records request, the burden is on the custodian to redact PII and other non-public, Confidential Data. G.S. § 132-6(c). Organizational Users must take all reasonable efforts to protect PII and other non-public, Confidential Data.

6.13 Restrictions on the Use of NCAOC-Issued Equipment

NCAOC-issued Information Technology Resources (including laptops, mobile devices) may not be taken outside of the United States without an exception that has been first approved by the requesting Organizational User's Hiring Authority and then by the NCAOC Director or CTO or his/her designee.

6.14 Restrictions on the Access of NCAOC Services and Judicial Branch Data

The NCAOC's services and Data may not be accessed from outside of the United States without an exception that has been first approved by the requesting Organizational User's Hiring Authority and then by the NCAOC Director or the CTO or his/her designee.

6.15 Retention of Records

a. Records in the legal custody of the clerks of superior court, including without limitation all case files and other Records of court proceedings, must be retained in compliance with the Rules of Recordkeeping and the Records Retention and Disposition Schedules for Clerks of Superior Court located respectively at: https://juno.nccourts.org/policies/judicial-branch/rules-recordkeeping-procedures-office-clerk-superior-court and https://juno.nccourts.org/policies/judicial-branch/records-retention-and-disposition-schedule.

b. Otherwise, Organizational Users are responsible for retaining Records in compliance with the Functional Schedules approved by the Department of Natural and Cultural Resources located at: https://archives.ncdcr.gov/government/state-government-agencies/functional-schedule.

6.16 Cybersecurity and Privacy Incidents

Any Event involving a stolen NCAOC-issued computing device, suspected or actual Cybersecurity Incident, Privacy Incident, Privacy Breach, or Security Breach (including unauthorized access) involving the security of networks, NCAOC Information Systems, applications, or computer systems, or Data requires immediate reporting to the NCAOC Help Desk at (919) 890-2407.

7 Compliance

Failure to adhere to this policy may put Information Technology Resources at risk. Sanctions for violation of this policy will be governed by Section 10, Enforcement, of this policy.

The NCAOC may conduct periodic reviews to ensure Organizational Users' policy compliance.

8 Dissemination

This policy will be given to information technology personnel with responsibilities for implementing this policy and any associated procedures, guidelines, or plans, including existing personnel upon approval of this policy and new personnel during their initial training. This policy may also be posted to the Technology Reference section of the NCAOC intranet for other Organizational Users. Affected Organizational Users will be notified of amendments to this policy through training and intranet announcements.

9 References

NIST Special Publications 800-53, r5
NCAOC Planning Policy
NCAOC Planning Procedures
NCAOC Data Classification Policy
G.S. § 143-805
G.S. § 132-1.10
G.S. § 14-190.13
G.S. § 7A-109(d)
G.S. § 132-6

10 Enforcement

This policy will be enforced by the CTO, the NCAOC Executive Management Team, Hiring Authorities, or court or judicial officials. Violations may result in disciplinary action(s), which may include a restriction or revocation of access privileges; a written warning or written reprimand; demotion; suspension without pay; dismissal; civil liability; and/or prosecution for applicable criminal violations. Where illegal activities or theft of Judicial Branch property (physical, electronic, or intellectual) are suspected, the Judicial Branch will report such activities to the applicable authorities.

11 NIST Controls Satisfied

Policy statements that satisfy the requirements of NIST controls as identified in Special Publication 800-53, r5, as revised are so indicated throughout this policy.

This policy in its entirety satisfies the requirements of the following control(s): **PL-4**.

12 Review Cycle

This policy shall be reviewed biennially by the Information Security Office. If changes to this policy are required prior to this biennial period, an ad hoc review will be performed.

13 Policy Approval

This policy has been reviewed and is hereby approved by the undersigned. The signed version of this policy will be stored by the CTO or the CTO's designee.

Chief Technology Officer

(Signature) *Anthony Whitmore* (Date) 6/2/25

(Printed name) Anthony Whitmore

14 Revision History

Change#	Date of Change	Effective Date	Revision Summary	Approval By (Initials)	Ver#
1	02/21/2019	02/21/2019	Final Version	MRW	v.3.4
2	11/05/2019	11/05/2019	Ad Hoc Review	MW	v.3.5
3	11/19/2019	11/19/2019	Ad Hoc Review	MW	v.3.6
4	12/17/2019	12/17/2019	Ad Hoc Review	MW	v.3.7
5	11/17/2021	01/26/2022	Annual Review	AW	v.3.8
6	03/02/2022	03/03/2022	Ad Hoc Review	AW	v.3.9
7	04/20/2022	06/07/2022	Ad Hoc Review	AW	v.3.10
8	08/09/2022	08/11/2022	Ad Hoc Review	AW	v.3.11
9	05/23/2023	05/31/2023	Ad Hoc Review	AW	v.3.12
10	07/30/2024	12/11/2024	Ad Hoc Review	AW	v.3.13
11	03/03/2025	06/03/2025	Ad Hoc Review	AW	v.3.14