Privacy and Security Requirements for Criminal Justice Agencies' Inquiry-Only Access to eWarrants and Judicial Branch Data

Prepared by
Technology Services Division | Information Security Office
May 2024

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. **DEFINITIONS**

a) "AGENCY" means the governmental Criminal Justice Agency that is qualified under Section 2.1 of the Agreement and is entering into the Agreement with the NCAOC.

b) "Agency Contact Form" means the Agency Contact and Information form attached to the Agreement as Attachment A.

c) "Agreement" means the document entitled "Authorized User Agreement With Criminal Justice Agencies For Inquiry-Only Access To eWarrants and Judicial Branch Data" in which these Privacy and Security Requirements and the Agency Contact Form are incorporated by reference.

d) "Authorized eWarrants User" means an employee of the AGENCY authorized by the NCAOC to have Inquiry-Only Access to eWarrants and Judicial Branch Data in accordance with the terms and conditions of the Agreement, including these Privacy and Security Requirements and the Agency Contact Form.

e) "Authorized Liaison" means a designee of an AGENCY Authorized Signatory, who has been given authority by the AGENCY Authorized Signatory to manage access to eWarrants for the AGENCY.

f) "Authorized Signatory" means an individual authorized to bind the AGENCY contractually or someone designated by him or her in writing. For state and federal agencies, the authorized signatory is the head of the agency (e.g., secretary or director) or someone designated in writing by him or her. For counties, the authorized signatory is the chairperson of a county board of commissioners or someone designated in writing by the board of commissioners. For municipalities, the authorized signatory is the mayor or equivalent office or someone designated by him or her.

g) "Computer" means a data processing device (including but not limited to a laptop, desktop, smartphone, tablet, etc.) capable of accepting data, performing prescribed operations on the data, and supplying the results of these operations. For Authorized eWarrants Users to access eWarrants or Judicial Branch Data, the AGENCY shall initially provide Authorized eWarrants Users' Computers with Microsoft Windows 10 (or later) and Microsoft Edge installed and shall comply with the requirements in these Privacy and Security Requirements and the Agreement.

h) "Confidential Judicial Branch Data" means a subset of Judicial Branch Data that is confidential or non-public information pursuant to applicable law, including Unreturned Warrant Information, Identifying Information, Personal Information, and Highly Restricted Personal Information, as those terms are defined below, as well as other data that is confidential or non-public under applicable law.

- "Unreturned Warrant Information" means all case information transmitted from eWarrants when the only filing in the case is an unreturned Warrant for Arrest or an unreturned Search Warrant. For cases in which there are other filings in addition to an unreturned Warrant for Arrest or an unreturned Search Warrant, Unreturned Warrant Information means only the case information related to the Warrant for Arrest or Search Warrant itself transmitted from eWarrants. Unreturned Warrant Information is classified by the Judicial Branch as Confidential Judicial Branch Data. No Unreturned Warrant Information shall be redisclosed by Authorized eWarrants Users except to Judicial Officials and employees of Public Law Enforcement Agencies who need to know the information to perform their

- official duties. Warrant information becomes public and may be redisclosed to other persons when the Warrant for Arrest has been returned to the clerks' office, notwithstanding whether the Warrant for Arrest has been served or not. See G.S. § 132-1.4(k).
- "Identifying Information" as used herein shall include the types of information included in the definition of "identifying information" in G.S. 132-1.10(b)(5) in addition to the other types of information listed below:
  - Social security or employer taxpayer identification numbers
  - Driver's license, State identification card, or passport numbers
  - Checking account numbers
  - Savings account numbers
  - Credit card numbers
  - Debit card numbers
  - Personal Identification (PIN) Code as defined in G.S. 14-113.8(6)
  - Digital signatures
  - Any other numbers or information that can be used to access a person's financial resources
  - Biometric data
  - Fingerprints
  - Passwords
  - FBI numbers
  - SBI numbers
  - Check digit numbers
  - Other information comprising non-public information as may be identified in applicable state or federal statutes, regulations, or other laws.
- "Personal Information" as used herein shall have the same meaning as in the DPPA, specifically 18 U.S.C. § 2725(3), which includes information obtained from a person's motor vehicle record that identifies an individual, including:
  - An individual's photograph
  - Social security number
  - Driver's identification number
  - Name
  - Address (but not the 5-digit zip code)
  - Telephone number
  - Medical or disability information.
- "Highly Restricted Personal Information" used herein shall have the same meaning as in the DPPA, specifically 18 U.S.C. § 2725(4), which includes information obtained from a person's motor vehicle record that identifies an individual, including:
  - An individual's photograph or image
  - Social security number
  - Medical or disability information.

i) "Criminal Justice Agency" means a court, a governmental agency, or any subunit of a governmental agency that performs the administration of criminal justice pursuant to a statute or executive order and allocates a substantial part of its annual budget to the administration of criminal justice, as defined in Section 3.2.4 the FBI's CJIS Security Policy, Version 5.9.1 (October 1, 2022).

j) "Effective Date" means the date of the last signature on the Agreement once fully executed.

k) "Electronic Warrants" or "eWarrants" shall mean Tyler's proprietary, cloud-based applications replacing NCAOC's legacy NCAWARE application.

l) "Information System" means a collection of multiple pieces of equipment involved in the collection, processing, storage, and dissemination of information such as a Computer, network equipment, hardware, software, and Computer system connections.

m) "IT Security Incident" includes a cybersecurity incident or significant cybersecurity incident as defined in G.S. § 143B-1320(a)(4a) and (16a), respectively, and any incident that is a violation of the North Carolina Identity Theft Protection Act, G.S. Chapter 75, Article 2A.

n) "Judicial Branch" means the North Carolina Judicial Branch.

o) "Judicial Branch Data" means the data provided to the AGENCY by or through direct, Inquiry-Only Access to eWarrants, which includes both Confidential Judicial Branch Data and public, non-confidential Judicial Branch Data.

p) "NCAOC" means the North Carolina Administrative Office of the Courts, which is the state agency within the Judicial Branch.

q) "Parties" refer jointly to the AGENCY and the NCAOC. "Party" refers to either one of the Parties.

r) "Priority Users" include judges, district attorneys, clerks of court, public defenders, magistrates, or NCAOC staff.

s) "Privacy and Security Requirements" mean this document, which is entitled "Privacy and Security Requirements for Criminal Justice Agencies' Inquiry-Only Access to eWarrants and Judicial Branch Data," referred to herein as "Privacy and Security Requirements," and incorporated by reference into the Agreement. These Privacy and Security Requirements are located at www.nccourts.gov (and any successor or related locations designated by the NCAOC) and may be updated by the NCAOC from time to time.

t) "Tyler" means Tyler Technologies, Inc., the third-party vendor with which the NCAOC has a contractual relationship to host Judicial Branch Data and provide eCourts applications, including eWarrants, to the NCAOC.

u) "Unauthorized Access, Use or Disclosure" means the unauthorized access to, or use of, eWarrants or Computing devices used by Authorized eWarrants Users or unauthorized access to, or disclosure or use of, confidential, non-public Judicial Branch Data.

v) "User Identifier" or "User ID" means an Authorized eWarrants User's unique identifier, which is used in conjunction with the Authorized eWarrants User's password to access eWarrants and Judicial Branch Data.

2. ACCESS to eWarrants

2.1 Authorized eWarrants User Identifier (ID) Requirements

a) The NCAOC shall provide Authorized eWarrants User IDs and temporary passwords to eligible individual users designated by the AGENCY who request access to eWarrants. The temporary password shall be changed by Authorized eWarrants Users immediately upon receipt to ensure their access is controlled and maintained.

b) Only the individual to whom an Authorized eWarrants User ID is uniquely associated shall use that ID. Sharing or generic use of an Authorized eWarrants User ID is prohibited.

c) An NCAOC-derived and -distributed Authorized eWarrants User ID shall be used only with eWarrants and not with other Information Systems or applications (such as home PCs, personal devices, banking, other Computer systems, or personal Internet service provider accounts such as Gmail) where unauthorized persons could obtain or use the Authorized eWarrants User ID.

d) Authorized eWarrants Users' IDs shall be decommissioned immediately when their access to eWarrants has been revoked.

e) If an Authorized eWarrants User ID is inactive for 90 days, the NCAOC will disable it.

f) An Authorized eWarrants User ID's activity in eWarrants may be logged and audited by the NCAOC and Tyler.

g) The AGENCY or its Authorized eWarrants Users recognize and hereby acknowledge that all Authorized eWarrants User IDs and passwords supplied by the NCAOC to the AGENCY are the property of the NCAOC and are classified by the NCAOC as "Confidential" Information," subject to the proprietary rights of the NCAOC. The AGENCY or its Authorized eWarrants Users agree to hold Authorized eWarrants User IDs and passwords in the strictest confidence. The AGENCY or its Authorized eWarrants Users further agree to exercise at all times the same care with respect to the Authorized eWarrants User IDs and passwords as the AGENCY or its Authorized eWarrants Users would exercise in the protection of the AGENCY's own confidential information.

h) The AGENCY acknowledges and agrees that the NCAOC may at any time, for any reason, delay, limit, or deny access to eWarrants or Judicial Branch Data (e.g., in the event the demand of Priority Users prevents further usage by Authorized eWarrants Users other than Priority Users). The NCAOC shall make reasonable efforts to provide the AGENCY with prompt written notice of the denial of access and the anticipated duration of such denial of access.

2.2 Password Requirements for All Authorized eWarrants Users

a) An Authorized eWarrants User's password for access to eWarrants shall not be revealed by anyone to anyone, including AGENCY supervisors and co-workers, family members, or even NCAOC personnel. The NCAOC or the AGENCY shall **never** contact an Authorized eWarrants User and ask for his or her password. Any person who asks for an Authorized eWarrants User's password while claiming to be "from the NCAOC or the AGENCY" shall be treated as an impostor.

b) If an Authorized eWarrants User is asked for his or her password for access to eWarrants, the Authorized eWarrants User shall report the event or IT Security Incident to the NCAOC immediately by calling the NCAOC Help Desk at 919-890-2407.

c) When creating a password, the AGENCY shall ensure its Authorized eWarrants Users meet or exceed the following password construction requirements specified in the **NCAOC Information System Password Requirements and Best Practices**:

1) Have a minimum length of eight (8) characters;

2) Not be a dictionary word or a proper name; and

3) Adhere to complexity requirements to ensure adequate strength by:

   i. Not containing all or part of the User account name;

   ii. Containing at least three (3) of the following categories:

      a. Upper case (A-Z);

      b. Lower case (a-z);

      c. Numeric character (0-9); or

      d. Special character (! @ # $ % & * _ + = ? / ~ ` ; : , < > | \ ). Special characters should not be used at the beginning or at the end of the password.

d) In addition to the password requirements and best practices above, it is recommended that Authorized eWarrants Users not include the following in their passwords:

   1) Confidential personal identifying information such as social security numbers, dates of birth, account numbers, driver's licenses, etc.;

   2) Names of family, pets, friends, co-workers, or fictional characters;

   3) Computer terms or names, commands, sites, companies, hardware, or software;

   4) The Authorized eWarrants User's company name, county, city, or any derivation thereof;

   5) Birthdays, addresses, phone numbers, or other personal information;

   6) Word or number patterns, like aaabbb, zyxwvuts, qwerty, or 123321;

   7) Any of the above spelled backwards;

   8) Any of the above preceded or followed by a digit (e.g., secret1 or 1secret); or

   9) Words that substitute letters with numbers to create dictionary words (e.g., g00db33f for goodbeef).

e) The AGENCY shall store all account information (e.g., Authorized eWarrants User IDs and passwords), as well as confidential Judicial Branch Data, in an encrypted format which complies with industry best practices.

f) Passwords must not be saved in files on computers or mobile devices without the use of an NCAOC Information Security Office-approved encryption or hashing algorithm. Authorized eWarrants Users should contact the NCAOC Help Desk for a list of approved options, if needed.

g) Password management software that allows Authorized eWarrants Users to maintain password lists or automated password inputs is prohibited, except for approved simplified/single sign-on systems.

h) An Authorized eWarrants User's password should not be stored in Internet browsers (e.g., Microsoft Edge or Google Chrome) that offer to "remember" passwords.

i) An Authorized eWarrants User's password should not be written down, displayed in clear text on a screen, or stored on any electronic media unless encrypted.

j) An Authorized eWarrants User's password shall not be changed in a cyclical nature (e.g., pass1, pass2, pass3, pass4, etc.).

k) An Authorized eWarrants User's password shall be changed at least every ninety (90) days.

3. AVAILABILITY and SUPPORT

3.1 Authorized eWarrants User Requirements

a) The AGENCY acknowledges and agrees to the following:

1) The timeframe within which eWarrants and Judicial Branch Data shall first become available for use by the AGENCY, through its Authorized eWarrants Users, shall be solely determined by the NCAOC. The NCAOC is not subject to any AGENCY implementation requirements or deadlines under the Agreement. The NCAOC shall make reasonable efforts to keep the AGENCY informed about implementation deadlines for the AGENCY.

2) The AGENCY and its Authorized eWarrants Users' rights under the Agreement, including these incorporated Privacy and Security Requirements, to gain access to eWarrants and Judicial Branch Data are subject to priority use by the Priority Users.

3) Subject to the availability of NCAOC staff and resources, limited help desk services and technical assistance may be extended to the AGENCY, and shall be provided to, or coordinated with, the contact persons listed in the AGENCY Contact Form. The telephone number for the NCAOC Help Desk is 919-890-2407.

4) The AGENCY shall designate one (1) or two (2) contact persons on the AGENCY Contact Form. Contact persons are the only individuals, in addition to the Signatory of the Agreement, who are permitted to contact the NCAOC on the AGENCY's behalf for any reason other than password resets for Authorized eWarrants User IDs. Only the Authorized eWarrants User to whom an ID has been assigned may call the NCAOC Help Desk to request a reset of his or her ID's password.

5) It is within the sole discretion of the NCAOC to delay the reset of the password for an Authorized eWarrants User ID for a reasonable time until NCAOC Help Desk staff are satisfied that a request for such reset has originated with the Authorized eWarrants User to whom the Authorized eWarrants User ID in question was assigned by the NCAOC. This verification process may include a demand for a written request from a contact person or the Signatory of the Agreement for reset of the password.

3.2 All Authorized eWarrants Users' Requirements

a) The AGENCY acknowledges and agrees to the following:

1) Should the NCAOC or Tyler experience a system outage or crash such that disaster recovery is activated, the AGENCY shall not have access to eWarrants or Judicial Branch Data. The AGENCY shall not be entitled to access eWarrants or Judicial Branch Data while the NCAOC or Tyler is operating eWarrants in disaster recovery mode.

2) The NCAOC may, at any time, delay, limit, or deny access to eWarrants or Judicial Branch Data to the AGENCY and its Authorized eWarrants Users for required maintenance. The NCAOC shall make reasonable efforts to provide the AGENCY with prompt notice of the denial of access and the anticipated duration of such denial of access.

3) The NCAOC's denial, refusal, or revocation of access to the AGENCY or its Authorized eWarrants Users shall not be considered a breach of the Agreement.

4. JUDICIAL BRANCH DATA PROTECTION REQUIREMENTS

a) The AGENCY or its Authorized eWarrants Users may have access to Confidential Judicial Branch Data. The AGENCY shall ensure that its Authorized eWarrants Users agree to maintain the strictest confidentiality of and carefully restrict access to eWarrants and Confidential Judicial Branch Data only as allowed in the Agreement, and to protect all from acquisition, loss, misuse, unauthorized disclosure, or breach pursuant to and as outlined herein and the Agreement.

b) The AGENCY, its Authorized eWarrants Users or any Vendor shall promptly refer any and all public records requests as follows:

1) Requests for Documentation shall be referred to the NCAOC.

2) Requests for Judicial Branch Data elements listed below shall be referred to the North Carolina Department of Transportation/Division of Motor Vehicles.

- Social security numbers
- Driver's license numbers
- Telephone numbers

3) All requests for Judicial Branch Data accessed within eWarrants shall be referred to the clerk of superior court in the county where the subject case is. The AGENCY recognizes and hereby acknowledges that the official custodian of all official court records for each county is the clerk of superior court of that county, and that the NCAOC is not the official custodian of any court records.

c) Judicial Branch Data accessed by the AGENCY or its Authorized eWarrants Users pursuant to the Agreement shall not be marketed or sold by the AGENCY or its Authorized eWarrants Users at any time, either during the term of the Agreement, or while the AGENCY or its Authorized eWarrants Users still have possession of Judicial Branch Data after the Agreement has terminated or expired. The ownership and custody of the Judicial Branch Data shall be unaffected by the exchange of Judicial Branch Data with the AGENCY or its Authorized eWarrants Users contemplated by these Privacy and Security Requirements and the Agreement.

d) The AGENCY or its Authorized eWarrants Users shall immediately report an Unauthorized Access, Use or Disclosure, IT Security Incident, defect, or downtime related to eWarrants to the NCAOC Help Desk by calling 919-890-2407. See Section 4.f).8) below for further direction regarding an IT Security Incident.

e) The AGENCY shall take full responsibility for maintaining and ensuring its Authorized eWarrants Users maintain the privacy, security, and confidentiality of Confidential Judicial Branch Data received from the NCAOC pursuant to and as outlined in these Privacy and Security Requirements and the Agreement. The AGENCY and its Authorized eWarrants Users shall observe all applicable federal and state laws for the use and protection of Confidential Judicial Branch Data provided under the Agreement. As a condition of continued access to eWarrants or Judicial Branch Data, the AGENCY shall ensure their Authorized eWarrants Users' successfully complete annual security awareness training, which shall cover key topics such as phishing, social engineering, and identifying and protecting confidential data.

f) To protect Judicial Branch Data, the AGENCY shall ensure its Authorized eWarrants Users use the following privacy safeguards to prevent unauthorized access to eWarrants or a use, disclosure, or transmission of confidential, non-public Judicial Branch Data other than as outlined in the Agreement or these Privacy and Security Requirements:

1) Refrain from disclosing confidential, non-public Judicial Branch Data to any unauthorized individual or entity, including a third party, who is not an Authorized eWarrants User as defined herein without prior written consent of the NCAOC or DOT/DMV, as applicable;

2) Monitor Authorized eWarrants Users' and their individual access to Confidential Judicial Branch Data elements, including Unreturned Warrant Information, Identifying Information, Personal Information, Highly Restricted Information, and any other information protected by applicable law;

3) Implement corrective action to eliminate or negate any harmful effect that is known of an Unauthorized Use, Access, Disclosure, or acquisition of Confidential Judicial Branch Data or to eWarrants in violation of the terms of the Agreement;

4) During the ordinary course of business, sanitize paper or storage media using the NIST 800-88, r1 clear method when the paper or the storage media that has stored Confidential Judicial Branch Data is no longer needed for business use or when it is necessary to destroy the paper or storage media in compliance with the AGENCY's data retention requirements. Removable media that cannot be sanitized using a NIST 800-88, r1 clear method (e.g., CD-Rs) must be physically destroyed using a NIST 800-88, r1 purge method.

5) Upon the revocation of access to eWarrants and Judicial Branch Data or termination of the Agreement:

i. Securely destroy/purge all Confidential Judicial Branch Data, including personally identifying information, CJI, social security numbers, driver's license numbers, Unreturned Warrant Information, received from the NCAOC in all forms in a secure manner; and

ii. Permanently delete all Confidential Judicial Branch Data from the AGENCY's databases, any storage media (e.g., hard drives or flash drives) used with Computers accessing eWarrants when the storage media are no longer part of a Computer accessing eWarrants, electronic files, or paper files (including backups) so no Confidential Judicial Branch Data is recoverable in any locations, adhering to NIST Special Publication (SP) 800-88 Revision 1, Guideline for Media Sanitation found at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf, and retain no copies of such confidential, non-public Judicial Branch Data. The AGENCY shall certify in writing within thirty (30) calendar days of such destruction/purge of confidential, non-public Judicial Branch Data that all Judicial Branch Data received by the AGENCY or its Authorized eWarrants Users have been destroyed/purged; and

iii. Return Judicial Branch Data in paper form to the NCAOC, or if requested by the NCAOC, delete or destroy the Judicial Branch Data (in paper or electronic form) in compliance with Section 4.f).5) above.

a. Until the AGENCY has certified completion of the return/destruction/purge of all Judicial Branch Data in accordance with the requirements outlined above in Section 4.f).5), the AGENCY, its Authorized eWarrants Users shall continue to comply with

all Judicial Branch Data Protection Requirements in this Section 4 even after the Agreement has terminated or expired.

6) The AGENCY or its Authorized eWarrants Users shall not take any action that would compromise the integrity or effectiveness of or security measures of eWarrants, Judicial Branch Data. Should the NCAOC determine that such compromise has occurred, the NCAOC may take such timely action to remedy the problem as it may determine in its reasonable judgment is required and either provide notification to the AGENCY or follow Section 4.f).7).

7) **Revocation of AGENCY Access**

i. **Immediate Revocation**. Unless otherwise provided for in the Agreement, the NCAOC may immediately, and without prior notice, revoke the AGENCY's Authorized eWarrants Users' access to eWarrants or Judicial Branch Data and cease access if it discovers or has a reasonable belief that the AGENCY or its Authorized eWarrants Users has breached any provision of the Agreement, including these Privacy and Security Requirements, or has violated any applicable law. If the NCAOC revokes access under this provision, the NCAOC agrees to notify the current AGENCY Contact Person identified in the AGENCY Contact Form of the NCAOC's revocation with all due haste, and as allowable, within three (3) business days of the revocation. If the NCAOC revokes access under this provision, the AGENCY or its Authorized eWarrants Users shall cease all use of eWarrants, confidential, non-public Judicial Branch Data to which they have access or are already in their possession.

In its sole discretion, the NCAOC may allow the AGENCY to resolve the issue that caused the revocation before terminating the Agreement. If, in its sole discretion, the NCAOC is satisfied that the ground for the immediate revocation has been resolved, the NCAOC may withdraw the revocation and allow access to eWarrants and Judicial Branch Data to continue. The NCAOC, however, shall not waive its right to terminate the Agreement if it chooses not to move forward with the immediate revocation.

If, in its discretion, the NCAOC is not satisfied that the ground for the immediate revocation has been resolved within a time period specified by the NCAOC in its notice, the NCAOC may request the AGENCY or its Authorized eWarrants Users destroy/purge all confidential, non-public Judicial Branch Data as outlined above in Section 4.f).5) and terminate the Agreement.

ii. **Non-Immediate Revocation**. In its sole discretion, the NCAOC may find that a single breach of these Privacy and Security Requirements, the Agreement, or a pattern of low risk breaches of these Privacy and Security Requirements or the Agreement, does not rise to an IT Security Incident or a level requiring immediate revocation of access to eWarrants or Judicial Branch Data. If so, the NCAOC agrees to notify the AGENCY Contact Person identified in the AGENCY Contact Form. If, in its discretion, the NCAOC is satisfied that the ground for the non-immediate revocation has been resolved within a time period specified by the NCAOC in its notice, the NCAOC may withdraw its decision to revoke access and allow continued access to eWarrants, System, or Judicial Branch Data. The NCAOC, however, does not waive the right to terminate the Agreement if it chooses not to move forward with the non-immediate revocation. If, in its discretion, the NCAOC is not satisfied that its concerns have been resolved in a timely fashion, the NCAOC may terminate the Agreement and revoke and deny access to eWarrants or Judicial Branch Data until such concerns have been resolved and a new

agreement has been signed.

8) **Incident Reporting, Breach, and Notification**

i. In the event of theft or loss of a Computer that allows access to Judicial Branch Data, the NCAOC Help Desk will be notified by the AGENCY or its Authorized eWarrants Users within twenty-four (24) hours of the theft or loss. The NCAOC and AGENCY will confirm mitigation of the associated risk (including changing passwords, restricting access, confirming whole disc encryption was installed and confirming that no Judicial Branch Data was stored on the lost or stolen Computer's hard drive).

ii. Additionally, in the event an AGENCY's Computer with access to the NCAOC network is infected with malware (e.g., Computer virus, trojan application, etc.), the AGENCY or its Authorized eWarrants Users must notify the NCAOC Help Desk immediately to provide risk mitigation instructions and to limit access for that device from the rest of the NCAOC network to prevent the spread of malware.

iii. In the event an IT Security Incident involving eWarrants or confidential, non-public Judicial Branch Data occurs, the AGENCY or its Authorized eWarrants Users shall comply with the following:

a. Notify the NCAOC Help Desk by calling (919) 890-2407 as quickly as possible of an IT Security Incident in a time frame not to exceed twenty-four (24) hours of discovery or notification of the IT Security Incident, by notifying and complying with their internal cybersecurity incident response policy. At a minimum, such notification shall contain, to the extent known: the nature of the IT Security Incident; specific information about the Judicial Branch Data compromised; the date the IT Security Incident occurred; the date the AGENCY or its Authorized eWarrants Users discovered or were notified of the IT Security Incident; and the identity of any applications impacted by the IT Security Incident and any affected or potentially affected individual(s). After the AGENCY provides the initial notification to the NCAOC, the AGENCY shall provide the NCAOC updated information regarding the status of the IT Security Incident weekly, at a minimum, until the IT Security Incident has been mitigated or resolved, or all affected individuals have been notified, whichever is latest.

b. The Parties shall work collaboratively to resolve the IT Security Incident, mitigate any damages, and notify any affected individuals.

c. If a notification to affected individuals is required under any law/regulation, pursuant to the NCAOC's policies, or if providing notification is in the best interests of the State, then notification to all persons and entities affected by the IT Security Incident (as reasonably determined by the NCAOC) shall be required. The AGENCY shall bear the cost of resolving the IT Security Incident, including the cost of the notification ("IT Security Incident Related Costs").

d. The AGENCY agrees to reimburse the NCAOC for all IT Security Incident Related Costs involving eWarrants, Judicial Branch Data. IT Security Incident Related Costs shall include the NCAOC's internal and external costs associated with addressing and responding to the IT Security Incident, including but not limited to: (a) preparation and mailing or other transmission of legally required notifications; (b) preparation and mailing or other transmission of such other

communications to customers, agents, or others as the NCAOC deems reasonably appropriate; (c) establishment of a call center or other communications procedures in response to such IT Security Incident (e.g., customer service FAQs, talking points, and training); (d) public relations and other similar crisis management services; (e) legal and accounting fees and expenses associated with the NCAOC's investigation of, and response to, such event; and (f) costs for credit reporting services that are associated with legally required notifications or are advisable, in the NCAOC's opinion, under the circumstances.

e. Upon the NCAOC receiving notification of an IT Security Incident, the NCAOC may, in its discretion, follow Section 4.f).7) above. Regardless of whether access is revoked, the AGENCY shall be required to cure the IT Security Incident within the time period specified by the NCAOC, or if the Agreement is terminated, the AGENCY agrees to complete an investigation to resolve the IT Security Incident and mitigate any vulnerability to eWarrants or Judicial Branch Data.

f. The management of and liabilities associated with securing and protecting eWarrants, and Judicial Branch Data provided to the AGENCY or its Authorized eWarrants Users is the responsibility of the AGENCY. The NCAOC is not responsible for IT Security Incidents involving the use, transmission, disclosure, or storage of Judicial Branch Data and access and use of eWarrants by the AGENCY or its Authorized eWarrants Users. The AGENCY will not be responsible for IT Security Incidents caused solely by acts or omissions by the NCAOC, Tyler, or NCAOC contractors.

9) **Information Security Requirements**

i. The AGENCY shall adhere to one (1) of the following information security requirements:

a. DIT's Statewide Information Security Manual and Security Policies; or

b. The AGENCY's security policies that address all applicable CJIS, NIST 800-53B High baseline, NIST Cybersecurity Framework, or comparable control framework requirements, **and** meet or exceed any security control requirements defined therein.

ii. Only AGENCY-owned and -supported Computers, software, and secure network connectivity shall be used by their Authorized eWarrants Users to access Judicial Branch Data. The AGENCY shall maintain said Computers and Information Systems in accordance with the Agreement and these Privacy and Security Requirements.

iii. The sole means by which the AGENCY, through its Authorized eWarrants Users, shall access and use eWarrants shall be by accessing and using eWarrants in the manner provided by the NCAOC under this agreement.

iv. The AGENCY shall install and maintain updated anti-virus software on all its Computing devices accessing eWarrants on the NCAOC network, or sharing removable media with Computers accessing eWarrants or Judicial Branch Data on the NCAOC network.

v. The AGENCY shall install and maintain updated anti-virus software on all its Computing devices accessing the NCAOC network or sharing removable media with Computers accessing the NCAOC network.

vi. The AGENCY shall install and maintain up-to-date security patches, security scanning tools, and firewalls in accordance with this Section 4.f).9) to maintain the privacy and security of Judicial Branch Data, and the AGENCY's Information Systems.

vii. The AGENCY shall implement and maintain internal data security measures, physical safeguards, access controls, and other security methods utilizing appropriate hardware and software necessary to monitor, maintain, and ensure Judicial Branch Data confidentiality in accordance with these Privacy and Security Requirements, the Agreement, or all applicable state or federal laws.

viii. The AGENCY shall restrict access to any processing environment storing confidential, non-public Judicial Branch Data unless the need for access complies with terms of the Agreement, including these Privacy and Security Requirements.

ix. The AGENCY shall ensure confidential, non-public Judicial Branch Data is secured in the AGENCY's environment, including but not limited to Computer or Information Systems maintained by the AGENCY or any third parties working on behalf of the AGENCY.

x. The AGENCY shall implement and maintain all appropriate administrative, physical, technical, and procedural safeguards at all times during the term of the Agreement to secure and maintain the privacy and security of such Judicial Branch Data from breach, protect the Judicial Branch Data from loss, Unauthorized Use, Access or Disclosure, and from hacks and other forms of malicious or inadvertent acts which could compromise the Judicial Branch Data.

xi. The AGENCY shall provide reasonable care and efforts to detect fraudulent activity involving the Judicial Branch Data in the AGENCY's infrastructure environment.

xii. The NCAOC specifically reserves the right, at its sole discretion, to alter operating hours, Computer applications (including eWarrants), connection methods, support services, equipment and software requirements, security requirements, and network services at any time and without prior notice to the AGENCY or its Authorized eWarrants Users.

10) **Infrastructure and Asset Security**

i. The AGENCY shall ensure it only processes, stores, or transmits Judicial Branch Data on Information Systems that leverage a standard baseline configuration that incorporates standard privacy and security protections such as:

a. preventing "administrative" access rights for non-IT administrator end users;

b. implementing Computer session timeouts.

ii. The AGENCY shall ensure all Computers accessing eWarrants or Judicial Branch Data will be restricted to Authorized eWarrants Users only. Portable or laptop Computers shall be kept in locked, secured locations or in the possession of the Authorized eWarrants User at all times. Authorized eWarrants Users shall not leave a Computer unattended when logged into eWarrants, which may allow unauthorized personnel to use their Computer or their Authorized eWarrants User ID to access eWarrants or Judicial Branch Data.

11) **Vulnerability Scanning and Patch Management**

i. The AGENCY shall ensure it reviews all devices accessing Judicial Branch Data monthly for current vulnerability and patch information.