Privacy and Security Requirements For Access to Judicial Branch Data and eCourts Applications

Prepared by
Technology Services Division | Information Security Office
September 30, 2021

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) "Addendum" means the document entitled "Addendum for Judicial Branch Data Sharing" and its appendices, in which these Privacy and Security Requirements are incorporated by reference.

b) "Addendum Effective Date" means the date of the last signature on the Addendum once fully executed and the date the Addendum is incorporated by reference into the Agreement.

c) "AGENCY" means the law enforcement agency which is qualified under Section 2.1 of the Agreement and is entering into the Agreement with the NCAOC.

d) "AGENCY Application" means the AGENCY's RMS that will share Judicial Branch Data with the eCourts Application(s) and receive and utilize Judicial Branch Data.

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

f) "Agreement" means the document entitled "Authorized User Agreement With Law Enforcement Agency For Access To eCourts Applications And Judicial Branch Data," in which these Privacy and Security Requirements and the Agency Contract Form are incorporated by reference, and the executed Addendum is incorporated by reference on the Addendum Effective Date.

g) "Applications" refer jointly to one or more eCourts Application(s) and the AGENCY Application, as those terms are defined herein.

h) "Authorized eCourts Application User" means an employee, official, or agent of the AGENCY authorized by the NCAOC to access and use eCourts Application(s), Judicial Branch Data, and Documentation in accordance with the terms and conditions of the Agreement, including these Privacy and Security Requirements and the Agency Contact Form.

i) "Authorized Liaison" means a designee of a Hiring Authority, who has been given authority by the Hiring Authority to manage access for the AGENCY.

j) "Authorized Users" means a named employee of the State or local Government entity in North Carolina, Tyler, or any Vendor, who is authorized to access the eCourts Application(s), Documentation, Judicial Branch Data, AGENCY Application, any Other AGENCY Applications, or the System to perform work for the purposes set forth in the Agreement or the Addendum. There are only three (3) types of Authorized Users, specifically, Authorized eCourts Application Users, Authorized Judicial Branch Data Users. and Authorized Technical Team Users, as these terms are defined in Section 1(h) of these Privacy and Security Requirements and Sections 5.2.1 and 5.2.2 of the Addendum, respectively.

k) "Brazos" means Tyler's proprietary, cloud-based, electronic citation solution replacing the NCAOC's in-house developed eCitation application.

l) "CJI" means criminal justice information owned and provided for use by the State of North Carolina by CJIS. CJI is subject to specific data compliance requirements.

m) "CJIS" means the Criminal Justice Information Services, a division of the FBI, that provides criminal justice and law enforcement agencies on the local, state, and federal levels access to CJIS databases for information (i.e., CJI) necessary to apprehend lawbreakers, perform background checks and track criminal activity.

n) "Computer" means a data processing device capable of accepting data, performing prescribed

operations on the data, and supplying the results of these operations. For Authorized eCourts Application Users to access eCourts Application(s) or Judicial Branch Data, the AGENCY shall initially provide Authorized eCourts Application Users' Computers with Windows 10 (or later) and Internet Explorer 11 (or later) installed and shall comply with the requirements in these Privacy and Security Requirements and the Agreement or Addendum.

o) "Documentation" means any online or written documentation related to the use or functionality of the eCourts Application(s) that Tyler provides or otherwise makes available to the NCAOC for its use and from the NCAOC to its Authorized eCourts Application Users, including instructions, user guides, manuals, and other training or self-help documentation.

p) "DPPA" means the federal Driver's Privacy Protection Act (18 U.S.C. §§ 2721, et seq.), which classifies data as Personal Information and Highly Restricted Personal Information. This definition shall also include North Carolina's companion statute: G.S. § 20-43.1.

q) "eCitation" means the NCAOC's-in-house developed application for electronic citations which shall be retired when Brazos is implemented.

r) "eCourts Applications" or eCourts Application(s)" means Tyler's Brazos, eWarrants, or Odyssey solutions that Authorized Tyler Application Users will access or that will share Judicial Branch Data with the AGENCY Application.

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

t) "Electronic Warrants" or "eWarrants" shall mean Tyler's proprietary, cloud-based solution replacing NCAWARE. eWarrants includes components of the Odyssey suite together with Tyler's customized components developed to replace NCAWARE's functionality.

u) "FBI" means the Federal Bureau of Investigation.

v) "Governmental entity" means an autonomous public agency, established by constitution, statute, or ordinance for a specified public purpose. Examples include North Carolina state agencies outside the Judicial Branch, member institutions of the North Carolina university system and community college system, county and local governments and their subdivisions, any of the preceding from other states, and agencies of the United States government.

w) "Highly Restricted Personal Information" as defined in 18 U.S.C. § 2725(4) means an individual's photograph or image, social security number, medical or disability information, and motor vehicle record.

x) "Hiring Authority" means the individual who supervises the staff of an AGENCY. The Hiring Authority for a Governmental entity is specified by the creating constitution, statute, ordinance, or charter.

y) "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.

z) "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.

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

bb) "Judicial Branch Data" means the data provided to the AGENCY by or through direct access to the eCourts Application(s) in the Agreement and for use in the AGENCY Application or any

Other AGENCY Applications for the authorized purposes set forth in the Addendum. The AGENCY will have access to Judicial Branch Data classified per the NCAOC's Data Classification and Handling Policy as "Public", "Confidential" or "Highly Confidential."

cc) "Non-governmental entity" means any individual or agency not included in the above definition of a "Governmental entity."

dd) "Nonprofit" means the status belonging to an entity incorporated under section 501(c)(3) of the Internal Revenue Code. For purposes of these Privacy and Security Requirements and the Agreement, a nonprofit acting on behalf of a Governmental entity is subject to the same requirements as a Governmental entity.

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

ff) "NCAWARE" means the NCAOC's in-house developed application for warrants and other criminal process forms and Judicial Branch Data which shall be retired when eWarrants is implemented.

gg) "Odyssey" means Tyler's proprietary, cloud-based, integrated case management solution being implemented for the Judicial Branch.

hh) "ORI" means an Originating AGENCY Identification assigned by the FBI.

ii) "Other AGENCY Applications" mean a data warehouse or other AGENCY application(s) or database(s) identified in Appendix C to the Addendum, over which the AGENCY has operational authority, direction, and control that may interface with, receive, or utilize Judicial Branch Data from the Agency Application.

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

kk) "PII" or "Personally Identifiable Information" includes any information identified in G.S. § 14-113.20(b) to the extent such information is excluded from public disclosure as required under the North Carolina Public Records Act or other law, and similar information comprising non-public information as may be identified in state or federal statutes, regulations or other laws.

ll) "Personal Information" as defined in 18 U.S.C. § 2725(3) means information 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, and medical or disability information.

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

nn) "Privacy and Security Requirements" mean this document, which is entitled "Privacy and Security Requirements for Access to eCourts Application(s) and Judicial Branch Data," and incorporated by reference into the Agreement and the Addendum. 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.

oo) "Public Law Enforcement Agency", as defined in G.S. § 132-1.4(b)(3), means a municipal police department, a county police department, a sheriff's department, a company police agency commissioned by the Attorney General pursuant to G.S. 74E-1, et seq., and any State

or local agency, force, department, or unit responsible for investigating, preventing, or solving violations of the law.

pp) "RMS" means the AGENCY's record management system.

qq) "Signatory" means the individual authorized to sign the Agreement or Addendum on an AGENCY's behalf for access to eCourts Application(s), Judicial Branch Data, or Documentation.

rr) "System" means the software, portal, platform, or other electronic medium controlled or utilized by the AGENCY or the NCAOC to exchange or access Judicial Branch Data in support of data sharing between the Applications.

ss) "Transfer Method" means the secure transfer method(s) the Parties mutually agree to use to transfer Judicial Branch Data from the eCourts Application(s) to the AGENCY Application and from the AGENCY Application to any Other AGENCY Applications. Examples of secure Transfer Methods include, without limitation, the following:

1) **API**: An Application Programming Interface defines interactions between multiple software intermediaries without any user involvement, including the kinds of programming calls or requests that can be made, how to make them, and the data formats that should be used. In practice, an API can use any protocols or design styles, be on- or off-line, and support XML and JSON.

2) **FTPS**: File Transfer Protocol over SSL (secure sockets layer) has two security modes, implicit and explicit. Implicit SSL requires the SSL connection to be created before any data transfer can begin. With explicit SSL, the negotiation takes place between the sender and receiver to establish whether data will be encrypted or unencrypted. This means confidential data or credentials can be set to require an encrypted connection before they will be shared. Like SFTP, the FTPS protocol can use a second factor of authentication for added security.

3) **HTTPS**: Hypertext Transfer Protocol Secure adds security to HTTP by offering certificate authentication. Additionally, it encrypts a Website's inbound traffic and introduces an encryption layer via transport layer security (TLS) to ensure data integrity and privacy.

4) **IPsec/VPN**: Internet Protocol Security is a secure network protocol suite that authenticates and encrypts data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).

5) **SFTP**: Secure File Transfer Protocol allows organizations to move data over a Secure Shell (SSH) data stream, providing excellent security over FTP. SFTP prevents unauthorized access to confidential data, including passwords, while data is in transit. The connection between the sender and receiver requires the user to be authenticated via a user ID and password, SSH keys, or a combination of the two.

6) **Web services:** A Web service is a collection of open protocols and standards which are widely used for exchanging data between systems or applications over the internet. Web services represent pure data interfaces typically delivered over HTTPS and are typically synchronous in nature, providing real time (current) data to consumer applications. A Web service can utilize three styles - REST, SOAP, and XML-RPC - for communication, and can support XML. Every web service is an API — since it exposes an application's data and/or functionality — but not every API is a web service.

tt) "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 Application(s) to the NCAOC for use by the Judicial Branch and, if the Addendum is executed by the NCAOC and the AGENCY, transmit Judicial Branch Data to the AGENCY Application for the purposes set forth in Section 3 of the Addendum.

uu) "Unauthorized Access, Use or Disclosure" means the unauthorized access to, use of or disclosure of the Applications, any Other AGENCY Applications, the System, Judicial Branch Data, Documentation or Computing devices used by Authorized Users.

vv) "Unreturned Warrant Information" means all case information transmitted from eCourts Application(s) when the only filing in the case is an unreturned Warrant for Arrest. For cases in which there are other filings in addition to an unreturned Warrant for Arrest, Unreturned Warrant Information means only the case information related to the Warrant for Arrest itself transmitted from eCourts Application(s). Unreturned Warrant Information is classified by the Judicial Branch as "Highly Confidential" Judicial Branch Data.

No Unreturned Warrant Information shall be disclosed except to Authorized Users in Public Law Enforcement Agencies. Warrant information may only be redisclosed to other Authorized Users when the Warrant for Arrest has been returned to the clerks' office, notwithstanding whether the Warrant for Arrest has been served or not.

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

xx) "Vendor" means any third-party vendor with which the AGENCY has, or may in the future have, a contractual relationship to host or manage Judicial Branch Data transferred from eCourts Application(s) to the AGENCY Application and if applicable, from the AGENCY Application to any Other AGENCY Applications for the purposes set forth in Section 3 of the Addendum.

2. ACCESS to APPLICATIONS and OTHER AGENCY APPLICATIONS

2.1 Authorized eCourts Application User Identifier (ID) Requirements

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

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

c) An NCAOC-derived and -distributed Authorized eCourts Application User ID shall be used only with eCourts Application(s) and not with other Information Systems or applications (such as a 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 eCourts Application User ID.

d) Authorized eCourts Application Users' IDs shall be decommissioned immediately when their access to eCourts Application(s) has been revoked.

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

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

g) Multi Factor Authentication (MFA) is required for direct access to an eCourts Application.

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

i) The AGENCY acknowledges and agrees that the NCAOC may at any time, for any reason, delay, limit, or deny access to eCourts Application(s), Judicial Branch Data, or Documentation in the event the demand of Priority Users prevents further usage by Authorized eCourts Application 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 Access Control Requirements for Authorized eCourts Application Users

a) Hiring Authorities and Authorized Liaisons will have delegated authority to manage access to eCourts Application(s) (request access or request termination of access) for Authorized eCourts Application Users using the NCAOC's MIM system. After receiving Hiring Authorities' or Authorized Liaisons' requests to grant access to or terminate access for an Authorized eCourts Application User, the MIM system will auto-provision the email and AD account for creation and then the NCAOC Access Administration Team will manually provision access to the requested eCourts Application(s). For terminating access, MIM will instantly disable the AD account and then the NCAOC Access Administration Team will remove the Authorized eCourts Application User's access to the eCourts Application(s).

b) As a part of the Hiring Authorities' or Authorized Liaisons' responsibilities, they shall request the NCAOC terminate access to the eCourts Application(s) for the Authorized eCourts Application User promptly (no later than 24 hours) when there is a change in the Authorized eCourts Application Users' employment or role status, such as when an:

   1) Authorized eCourts Application User transfers to a new role within the AGENCY where his or her prior access to the eCourts Application(s) is no longer necessary or required; or

   2) Authorized eCourts Application User separates from employment with the AGENCY

because of:

i. termination;

ii. retirement; or

iii. resignation.

3) The AGENCY needs to terminate an Authorized eCourts Application User's access to eCourts Application(s) for any reason other than the reasons included above in Section 2.2.b).1) or 2.2.b).2) above.

c) If a Hiring Authority or Authorized Liaison believes a separating Authorized eCourts Application User is a high risk to Judicial Branch Data, the Hiring Authority or Authorized Liaisons will be responsible for requesting immediate access termination of the Authorized eCourts Application User.

d) Hiring Authorities or Authorized Liaisons will ensure eCourts Application Users processing, storing or transmitting Judicial Branch Data leverage appropriate logical (software) controls on Computers they use to restrict unauthorized access to any downloaded Judicial Branch Data.

e) Hiring Authorities or Authorized Liaisons shall ensure that all Authorized eCourts Application Users accessing Judicial Branch Data under the Agreement have satisfactorily passed a background check prior to the NCAOC providing Authorized eCourts Application Users access to eCourts Application(s).

f) Hiring Authorities or Authorized Liaisons will ensure physical access to eCourts Application(s), which stores or processes Judicial Branch Data, is restricted to only Authorized eCourts Application Users.

g) If requested by the NCAOC, Hiring Authorities or Authorized Liaisons shall support NCAOC audits, including providing the NCAOC or an external auditor information or documents related to the AGENCY's access to eCourts Applications that Hiring Authorities or Authorized Liaisons manage.

2.3 Access Control Requirements for Addendum - Authorized Judicial Branch Users and Authorized Technical Team Users

a) The AGENCY or any Vendor, as a part of their responsibilities in the Addendum, shall also request the NCAOC terminate access to the AGENCY Application, any Other AGENCY Applications, or the System promptly (no later than 24 hours) when there is a change in the Authorized Judicial Branch Users' or Authorized Technical Team Users' employment or role status, such as when:

1) An Authorized Judicial Branch User or Authorized Technical Team User transfers to a new role within the AGENCY where his or her prior access to the AGENCY Application, any Other AGENCY Applications, or the System is no longer necessary or required; or

2) An Authorized Judicial Branch User or Authorized Technical Team User separates

from employment with the AGENCY because of:

i. termination;

ii. retirement; or

iii. resignation.

3) The AGENCY needs to terminate an Authorized Judicial Branch User's or Authorized Technical Team User's access to the AGENCY Application, any Other AGENCY Applications, or the System for any reason other than the reasons included above in Section 2.3.b).1) or 2.3.b).2) above.

b) If the AGENCY or any Vendor believes a separating Authorized Judicial Branch User or Authorized Technical Team User is a high risk to Judicial Branch Data, the AGENCY or any Vendor will be responsible for immediately terminating access of the Authorized Judicial Branch User or Authorized Technical Team User.

c) The AGENCY or any Vendor processing, storing or transmitting Judicial Branch Data will leverage appropriate logical (software) controls on Computers, the AGENCY Application or any Other AGENCY Applications to restrict unauthorized access to any downloaded Judicial Branch Data.

d) The AGENCY will ensure physical access to the AGENCY Application or any Other AGENCY Applications which store or process Judicial Branch Data, is restricted to only Authorized Judicial Branch Users or Authorized Technical Team Users.

e) If requested by the NCAOC, the AGENCY or any Vendor shall support NCAOC audits, including providing the NCAOC or an external auditor information or documents related to access to Judicial Branch Data that the AGENCY or any Vendor manages.

2.4 Password Requirements for All Authorized Users

a) An Authorized User's password for access to the Applications, any Other AGENCY Applications, Judicial Branch Data, or the System 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 User and ask for his or her password. Any person who asks for an Authorized User's password while claiming to be "from the NCAOC or the AGENCY" shall be treated as an impostor.

b) If an Authorized User is asked for his or her password for access to the Applications, any Other AGENCY Applications, Judicial Branch Data, or the System, the Authorized 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 Users meet or exceed password requirements specified in the NCAOC Information System Password Requirements and Best Practices or the password requirements specified in DIT's Statewide Security Manual. All passwords must conform to the following construction requirements:

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 Users not include the following in their passwords:

1) Confidential personal identifying information such as social security number, date of birth, account numbers, driver's license, 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 eCourts Application 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 eCourts Application 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 Information Security Office-approved encryption or hashing algorithm. Authorized Users should contact the IT Help Desk for a list of approved options, if needed.

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

h) An Authorized User's password should not be stored in Internet browsers (e.g., Internet Explorer® or Firefox)) that offer to "remember" passwords.

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

k) Except for Authorized Technical Team Users, an Authorized User's password shall be changed at least every ninety (90) days.

3. AVAILABILITY and SUPPORT

3.1 Authorized eCourts Application User Requirements

a) The AGENCY acknowledges and agrees to the following:

1) The timeframe within which the eCourts Application(s) and Judicial Branch Data shall first become available for use by the AGENCY, through its Authorized eCourts Application 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 eCourts Application Users' rights under the Agreement, including these incorporated Privacy and Security Requirements, to gain access to the eCourts Application(s) 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 eCourts Application User IDs. Only the Authorized eCourts Application 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 eCourts Application User ID for a reasonable time until NCAOC Help Desk staff are satisfied that a request for such reset has originated with the Authorized eCourts Application User to whom the Authorized eCourts Application 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 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 eCourts Application(s), Documentation, or Judicial Branch Data. The AGENCY shall not be entitled to access eCourts Application(s), Documentation, or Judicial Branch Data while the NCAOC or Tyler is operating the eCourts Application(s) in disaster recovery mode.

2) The NCAOC may, at any time, delay, limit, or deny access to eCourts Application(s), Documentation or Judicial Branch Data to the AGENCY, its Authorized Users and any Vendor 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, its Authorized Users, or any Vendor shall not be considered a breach of the Agreement or Addendum.

4. JUDICIAL BRANCH DATA PROTECTION REQUIREMENTS

a) The AGENCY, its Authorized Users, or any Vendor may have access to Documentation and confidential, non-public Judicial Branch Data. The AGENCY shall ensure that its Authorized Users and any Vendor agree to maintain the strictest confidentiality of and carefully restrict access to the Applications, any Other AGENCY Applications, Documentation, the System, and Judicial Branch Data to only Authorized Users, and to protect all from acquisition, loss, misuse, unauthorized disclosure, or breach pursuant to and as outlined herein and the Agreement or Addendum.

b) The following Judicial Branch Data elements in the eCourts Application(s) are obtained from the North Carolina Department of Transportation, Division of Motor Vehicles ("DOT/DMV"), and are protected from redisclosure by the Driver's Privacy Protection Act, 18 U.S.C. § 2721 et seq. ("the DPPA"):

1) Social security numbers;

2) Driver's license numbers;

3) Photographs or images;

4) Telephone numbers;

5) Medical or disability information; and

6) Email addresses.

c) These protected DPPA Judicial Branch Data elements continue to be in the legal custody of the DOT/DMV. The AGENCY is authorized to use these protected DPPA Judicial Branch Data elements exclusively for its internal, governmental purposes and shall not redisclose these protected DPPA Judicial Branch Data without the prior written consent of the DOT/DMV except to a Vendor insofar as the Vendor is acting on behalf of the AGENCY to perform its internal, governmental purposes. The AGENCY shall refer any requests for access to these protected DPPA Judicial Branch Data elements to the DOT/DMV.

d) The AGENCY, its Authorized Users, or any Vendor may have access to criminal justice information ("CJI") in Brazos and eWarrants. The AGENCY shall ensure all Authorized Users or any Vendor accessing CJI in Brazos or eWarrants are certified to access the CJI and shall comply with all applicable requirements in the FBI's current Criminal Justice Information Systems ("CJIS") Security Policy. By way of example, Brazos and eWarrants provide access to FBI numbers (also known as Universal Control Numbers) which, when coupled with personally identifying information, constitute protected CJI. *See the CJIS Security Policy, Section 4.1 at: https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.*

e) The AGENCY, its Authorized 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 in subsection 4.b) of these Privacy and Security Requirements shall be referred to the DOT/DMV.

3) All requests for Judicial Branch Data accessed within the eCourts Application(s) 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.

4) All requests for Judicial Branch Data accessed within the AGENCY Application or any Other AGENCY Applications, pursuant to the Addendum, shall comply with Section 7 of the Addendum.

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

g) The AGENCY, its Authorized Users, or any Vendor shall immediately report an Unauthorized Access, Use or Disclosure, IT Security Incidents, defects, or downtime related to the eCourts Application(s) to the NCAOC Help Desk by calling 919-890-2407. See Section 4.i).8) below for further direction regarding an IT Security Incident.

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

i) To protect Judicial Branch Data, the AGENCY shall ensure its Authorized Users or any Vendor use the following privacy safeguards to prevent unauthorized access to Applications, any Other AGENCY Applications, Documentation, or the System, or a use, disclosure, or transmission of Judicial Branch Data or Documentation other than as outlined in the Agreement, the Addendum, or these Privacy and Security Requirements:

1) Refrain from disclosing Judicial Branch Data or Documentation to any unauthorized individual or entity, including a third party, who is not an Authorized User as defined herein without prior written consent of the NCAOC;

2) Monitor Authorized Users' and their individual access to higher-risk Judicial Branch Data elements, such as personally identifying information, CJI, DPPA, Unreturned Warrant Information, juvenile data, adoption data, or special proceedings confidential data;

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

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 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 eCourts Application(s), the System, Judicial Branch Data or Documentation, or termination of the Agreement or Addendum:

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

   ii. Permanently delete all Judicial Branch Data from the AGENCY's or any Vendor's databases, any storage media (e.g., hard drives or flash drives) used with Computers accessing Applications or any Other AGENCY Applications when the storage media are no longer part of a Computer accessing Applications or any Other AGENCY Applications, electronic files, or paper files (including backups) so no 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 Judicial Branch Data. The AGENCY or any Vendor shall certify in writing within thirty (30) calendar days of such destruction/purge of Judicial Branch Data that all Judicial Branch Data received by the AGENCY, its Authorized Users or any Vendor have been destroyed/purged; and

   iii. Return Documentation in paper form to the NCAOC, or if requested by the NCAOC, delete the Documentation or destroy it (paper or electronic form) in compliance with Section 4.i).5) above.

      a. Until the AGENCY has certified completion of the return/destruction/purge of all Judicial Branch Data or Documentation in accordance with the requirements outlined above in Section 4.i).5), the AGENCY, its Authorized Users or any Vendor shall continue to comply with all Judicial Branch Data Protection Requirements in this Section 4 even after the Agreement or Addendum has terminated or expired.

6) The AGENCY, its Authorized Users or any Vendor shall not take any action that would compromise the integrity or effectiveness of the Information Systems or security measures of eCourts Application(s), Judicial Branch Data or Documentation. 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.i).7).

7) **Revocation of AGENCY or any Vendor Access**

   i. **Immediate Revocation**. Unless otherwise provided for in the Agreement or Addendum, the NCAOC may immediately, and without prior notice, revoke the AGENCY's Authorized Users' or any Vendor's access to the eCourts Application(s), the System, Judicial Branch Data, or Documentation and cease access if it discovers or has a reasonable belief that the AGENCY, its Authorized Users or any Vendor has breached any provision of the Agreement or Addendum, 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 or Section 12.11 of the Addendum (if different), 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, its Authorized Users or any Vendor shall cease all use of the eCourts Application(s), System, Judicial Branch Data or Documentation 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 or Addendum. 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 the eCourts Application(s), System, Documentation and Judicial Branch Data to continue. The NCAOC, however, shall not waive its right to terminate the Agreement or Addendum, 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, its Authorized Users or any Vendor destroy/purge all Judicial Branch Data or Documentation as outlined above in Section 4.i).5) and terminate the Agreement or Addendum.

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 Addendum, or a pattern of low risk breaches of these Privacy and Security Requirements, the Agreement or Addendum, does not rise to an IT Security Incident or a level requiring immediate revocation of access to the eCourts Application(s), System, Documentation, or Judicial Branch Data. If so, the NCAOC agrees to notify the Agency Contact Person identified in the Agency Contact Form or listed in Section 12.11 of the Addendum (if different). 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 the eCourts Application(s), System, Judicial Branch Data or Documentation. The NCAOC, however, does not waive the right to terminate the Agreement or Addendum, 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 or Addendum and revoke and deny access to the eCourts Application(s), System, Documentation, or Judicial Branch Data until such concerns have been resolved and a new agreement or addendum has been signed.

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

i. In the event of theft or loss of a Computer that allows unauthorized access to Judicial Branch Data or Documentation, the NCAOC Help Desk will be notified by the AGENCY, its Authorized Users or any Vendor within twenty-four (24) hours of the theft or loss, so the NCAOC can take actions to contain and mitigate the associated risk to the NCAOC (including changing passwords, restricting access, and confirming whole disc encryption is installed and no Judicial Branch Data or Documentation has been stored on the 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, its Authorized Users or any Vendor 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 the Applications, any Other AGENCY Applications, System, Documentation or Judicial Branch Data occurs, the AGENCY, its Authorized Users or any Vendor 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, its Authorized Users or any Vendor discovered or were notified of the IT Security Incident; and the identity of any Applications or Other AGENCY Applications impacted by the IT Security Incident; or 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. The AGENCY shall be responsible for obtaining information from its Vendor and providing it to the NCAOC.

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 the Applications, any Other AGENCY Applications, System, Judicial Branch Data or Documentation. 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.i).8) above. Regardless of whether access is revoked, the AGENCY or any Vendor shall be required to cure the IT Security Incident within the time period specified by the NCAOC, or if the Agreement or Addendum is terminated, the AGENCY agrees to complete an investigation, working with its Vendor, if necessary, to resolve the IT Security Incident and mitigate any vulnerability to the Applications, any Other AGENCY Applications, System, Documentation, or Judicial Branch Data.

f. The management of and liabilities associated with securing and protecting the Applications, Other AGENCY Applications, System, Judicial Branch Data and Documentation provided to the AGENCY, its Authorized Users or any Vendor 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 or Documentation and access and use of the Applications, any Other AGENCY Applications or System by the AGENCY, its Authorized Users or any Vendor. The AGENCY will not be responsible for IT Security Incidents caused by acts or omissions by the NCAOC, Tyler, or NCAOC contractors.

9) **Information Security Requirements**

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

a. The NCAOC's Policies;

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

c. The AGENCY's or any Vendor's security policies that address all applicable CJIS or NIST 800-53, r4 or higher controls **and** meet or exceed any NCAOC-specific security control requirements defined therein.

ii. The AGENCY or any Vendor shall install and maintain updated anti-virus software on all its Information Systems and Computing devices accessing the AGENCY Application, any Other AGENCY Applications, or System (which provide access to or store Judicial Branch Data) on its network, or sharing removable media with Computers accessing the AGENCY Application, any Other AGENCY Applications, System, or Judicial Branch Data on its network.

iii. 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.

iv. The AGENCY or any Vendor shall install and maintain up-to-date security patches, security scanning tools, and firewalls in accordance with this Section 4.i).9) to maintain the privacy and security of Judicial Branch Data, Documentation, the System, the AGENCY's Information Systems, AGENCY Application, and any Other AGENCY Applications.

v. The AGENCY or any Vendor shall log access to the AGENCY Application, any Other AGENCY Applications, and security events, and those logs shall be retained for a

minimum of one (1) year.

vi. The AGENCY or any Vendor shall ensure the AGENCY Application, any Other AGENCY Applications, and the System are audited for security on a regular basis.

vii. The AGENCY or any Vendor 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 and Documentation confidentiality in accordance with these Privacy and Security Requirements, the Agreement, the Addendum or all applicable state or federal laws.

viii. The AGENCY or any Vendor shall restrict access to any processing environment storing Judicial Branch Data or Documentation unless the need for access complies with terms of the Agreement or Addendum, including these Privacy and Security Requirements.

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

x. The AGENCY or any Vendor shall implement and maintain all appropriate administrative, physical, technical, and procedural safeguards at all times during the term of the Agreement or Addendum to secure and maintain the privacy and security of such Judicial Branch Data and Documentation from breach, protect the Judicial Branch Data and Documentation 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 or Documentation.

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

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

xiii. Only AGENCY- or Vendor-owned and -supported Computers, software, and secure network connectivity shall be used by their Authorized Users to access the Applications, any Other AGENCY Applications, the System, Documentation or Judicial Branch Data. The AGENCY or any Vendor shall maintain said Computers and Information Systems in accordance with the Agreement, the Addendum, and these Privacy and Security Requirements.

xiv. The sole means by which the AGENCY, through its Authorized eCourts Application Users, shall access and use eCourts Application(s) shall be by accessing and using the eCourts Application(s) provided by the NCAOC.

10) **Infrastructure and Asset Security**

i. The AGENCY shall ensure it or any Vendor only process, store, or transmit Judicial Branch Data or Documentation 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 and maintaining a strong encryption algorithm to encrypt all Judicial Branch Data at rest and leveraging a FIPS 140-2-approved Cryptographic module to protect all Judicial Branch Data and Documentation stored to Information Systems and other forms of media, including on mobile devices, to ensure the confidentiality of the Judicial Branch Data or Documentation; and

   c. implementing Computer session timeouts.

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

iii. Any Information System or Computing devices accessing the NCAOC network or processing or storing Judicial Branch Data or Documentation must comply with the following:

   a. Password-protect all access points to the NCAOC network; and

   b. Utilize encrypted communications (e.g., SSH), versus unsecure methods, such as telnet, for all remote management.

iv. All Computing devices with access to the AGENCY Application, any Other AGENCY Applications, System, Judicial Branch Data or Documentation, when not monitored directly, must have at least one (1) of the following controls performed after thirty (30) minutes of non-use (although there are some exceptions to this length of time):

   a. Authorized Users are automatically logged out of the AGENCY Application or any Other AGENCY Applications; or

   b. Authorized Users implement a password-protected screen saver on their Computers.

11) **Vulnerability Scanning and Patch Management**

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

ii. The AGENCY shall ensure it or any Vendor ensure the AGENCY Application or any Other AGENCY Applications that process, store, or transmit Judicial Branch Data is:

   a. periodically scanned for vulnerabilities consistent with either the NCAOC Vulnerability Management Guidelines or CJIS security policies.

b. patched consistent with the patching requirements in either DIT's Statewide Information Security Manual and Policies or those listed below.

1. Address Critical vulnerabilities within seven (7) calendar days of their detection or disclosure;
2. Address High vulnerabilities within thirty (30) calendar days of detection or disclosure;
3. Address Medium vulnerabilities within six (6) months of detection or disclosure; and
4. Address Low vulnerabilities within a reasonable time frame based on industry standards.

12) **Additional Data Protection Requirements for Data Sharing (Applies to Addendum Only)**

i. In addition to the requirements outlined above in Section 4.i).1)-11), the AGENCY, its Authorized Users, or any Vendor shall comply with the following when the NCAOC shares Judicial Branch Data with the AGENCY pursuant to an executed Addendum.

a. **Encryption in Transit:** The AGENCY shall implement encrypted transmissions using firewall protection or VPN (IPsec) for all servers hosting Judicial Branch Data such as TLS version 1.2 or later.

b. The AGENCY Application, any Other AGENCY Applications, or Information Systems that connect to the NCAOC network perimeter should also be protected with a firewall device/software.

c. The AGENCY or any Vendor shall ensure the AGENCY Application's connectivity to the eCourts Application(s) and the AGENCY Application's connectivity to any Other AGENCY Applications for the purpose of sending or receiving Judicial Branch Data (excluding email exchange) that traverse untrusted networks (e.g., the Internet) shall be encrypted using an encryption technology which complies with industry best practices (e.g., SSL, VPN, etc.).

d. Additional security measures (e.g., security tokens, Multifactor authenticator codes, digital certificates) entrusted to an Authorized User, the AGENCY, or any Vendor shall not be shared and will be protected with the same diligence as the eCourts Application User ID and password.

e. The AGENCY shall ensure the AGENCY's or any Vendor's facility(ies) hosting Judicial Branch Data maintains controlled access for its staff or third parties.

f. The AGENCY or any Vendor shall secure its network through monitoring by an Intrusion Detection Solution (IDS) for unauthorized access and provide remote support.

g. The AGENCY or any Vendor shall ensure a breach or compromise to another database server in the AGENCY's or any Vendor's infrastructure environment shall not subject the AGENCY Application, Other AGENCY Applications, System, Applications, or Judicial Branch Data to a breach or compromise.

h. At the NCAOC's request, the AGENCY shall allow the NCAOC to perform a vulnerability scan on the AGENCY's or any Vendor's communications Transfer

Method to ensure "transient trusts," including but not limited to, backdoors, cyber-threats, vulnerabilities, and unauthorized access, are prevented, and that due diligence is being performed in accordance with these Privacy and Security Requirements.

i. The AGENCY or any Vendor shall not create an unsecure entry into the Applications, any Other AGENCY Applications or the System.

j. The AGENCY or any Vendor shall restrict access to the Applications, any Other AGENCY Applications, the System or Judicial Branch Data according to role-based access controls that enforce the principles of least privilege and separation of duties.

k. The AGENCY shall ensure that any Vendor or any other third parties that access, create, receive, maintain, process, transmit, or store Judicial Branch Data on its behalf agree to the same restrictions and conditions that apply to the AGENCY with respect to such Judicial Branch Data.

l. In a virtualized environment, the AGENCY and any Vendor solution storing Judicial Branch Data shall be partitioned such that the AGENCY Application or Other AGENCY Applications and Judicial Branch Data shall be separated from and inaccessible to all individuals with no need for access.

m. The AGENCY shall ensure it or any Vendor stores and maintains all Judicial Branch Data securely in its or any Vendor's infrastructure environment.

n. In the event the Addendum is terminated or Judicial Branch Data is no longer able to be hosted or maintained by the AGENCY or any Vendor, the AGENCY shall ensure it or any Vendor complies with Section 4.i).5) above.

o. In any contract with a Vendor, the AGENCY shall include language retaining the AGENCY's or the NCAOC's right and ability to immediately secure and recover Judicial Branch Data free of any liens or other claims against such Judicial Branch Data in the event of a default or a proposed hosting change and require any Vendor to include this language in contracts with its vendors, subcontractors, or other hosting service providers.

p. The AGENCY or any Vendor shall prohibit remote access to, and the storage of, Judicial Branch Data from outside the continental United States, including, without limitation, remote access to Judicial Branch Data by authorized services support staff in identified support centers, since these actions are prohibited.

q. The AGENCY Application or any Other AGENCY Applications shall offer various levels of security, including, but not limited to, the following:

    1. Security controlled access to the AGENCY Application or any Other AGENCY Applications and Judicial Branch Data as well as security level restrictions on the access to functions, including inquiry-only functions;

    2. Strictly limit global access to all functions; and

    3. Restrict access to any processing environment storing Judicial Branch Data unless the need for access complies with terms of the Agreement or Addendum.

r. During the term of the Agreement or Addendum, the AGENCY agrees to notify the NCAOC of any amendments to agreement(s) between the AGENCY and any Vendor within thirty (30) days of the effective date of any such amendment or agreement if it would materially alter the System, Applications, Judicial Branch Data, or the AGENCY's, Authorized Users' or any Vendor's access to and collection, use, storage, or transmission of Judicial Branch Data.

s. Continuous Monitoring

1. The AGENCY shall ensure it or any Vendor complies with the NCAOC's continuous monitoring process to perform security/risk assessments on its AGENCY Application, any Other AGENCY Applications, or the infrastructure environment storing Judicial Branch Data using NIST 800-53, r4 controls to assess its compliance with enterprise security standards as outlined below. The AGENCY shall ensure it or any Vendor:

   (a) Completes a Third-Party Questionnaire and provides it to the NCAOC for review.

   (b) Provides a current copy of an industry-recognized third-party attestation of compliance(e.g., ISO 27001, SOC 2 Type 2, etc.) report for the AGENCY or any Vendor that:

      (1) will have logical or physical access to the AGENCY Application or any Other AGENCY Applications that store, process, or transmit Judicial Branch Data; or

      (2) could impact the privacy or security of the Judicial Branch Data, within thirty (30) calendar days after execution of the Addendum.

   (c) Annually, provides a new copy of such industry-recognized third-party attestation of compliance report (e.g., ISO 27001, SOC 2 Type 2, etc.) for the AGENCY or any Vendor.

2. The AGENCY or any Vendor (through the AGENCY) shall notify the NCAOC immediately if it decides to no longer host the AGENCY Application, any Other AGENCY Applications or Judicial Branch Data on premise within the AGENCY's or the same Vendor's environment.

3. The AGENCY or any Vendor shall provide corrective action plans or take immediate actions to resolve any exceptions, vulnerabilities, material weaknesses, and/or control deficiencies identified in the SOC 2, Type II report.

   If the AGENCY or any Vendor is unable to provide a current SOC 2, Type II report as required herein, but can provide a SOC 2, Type I report, the NCAOC will initially grant the AGENCY or any Vendor six (6) months to obtain and provide the NCAOC a SOC 2, Type II report if:

   (a) The AGENCY or any Vendor notifies the NCAOC that it is seeking a SOC 2, Type II report; and
   (b) The AGENCY or any Vendor is unable to conduct a SOC 2, Type II third-party assessment because of circumstances beyond the AGENCY's or Vendor's control (e.g., COVID-19).

The AGENCY or any Vendor shall notify the NCAOC in the event it cannot provide the SOC 2 Type II report within this initial six-month period and may request an additional extension, providing a justification to the NCAOC supporting its extension request. In its sole discretion, the NCAOC may grant the AGENCY or any Vendor an extension for up to six (6) months. The NCAOC's decision to grant the AGENCY or any Vendor an extension to submit its SOC 2, Type II report, however, shall not be construed to remove or limit the AGENCY's or any Vendor's obligation to comply with the requirements herein.