MEMORANDUM OF UNDERSTANDING

Regarding Access to the Comprehensive Outcome, Research, and Evaluation (CORE) Reporting System

I. PARTIES

This Memorandum of Understanding ("MOU") is entered into between the Wisconsin Department of Justice ("DOJ") and the Agency ("Site") specified in Section XVII below, for the purposes and uses, and on the conditions, set forth herein.

II. TERM

This MOU shall remain in effect through December 31, 2024, unless terminated pursuant to the provisions of Section XVI of this MOU.

III. DEFINITIONS

A. Authorized Representative means the individual designated by a site to execute this MOU and any associated Management Control Agreement (MCA). The authorized representative must have signing-authority to enter into such an agreement on behalf of the county or tribe, which in most cases would be the county executive, county board chair, county administrator, tribal administrator, or equivalent. Any other designation of an authorized representative must be approved in advance by WI DOJ.

B. BCS means the Bureau of Computing Services within WI DOJ's Division of Management Services.

C. BJIA means the Bureau of Justice Information and Analysis within the WI DOJ's Division of Law Enforcement Services.

D. BJIA Admin User means a CORE Reporting System administrative role reserved for BJIA employees. This role has the highest level of functionality of the CORE Reporting System. These users are employees of the WI DOJ.

E. Criminal Justice Agency means the courts or a governmental agency or any subunit thereof that performs the administration of criminal justice pursuant to a statute or executive order and that allocates a substantial part of its annual budget to the administration of criminal justice.

F. Confidential Information means all tangible and intangible information and materials accessed or disclosed in connection with this MOU and access to data in the CORE Reporting System, in any form or medium (and without regard to whether the information is owned by the State or by a third party), that satisfy at least one of the following criteria:

   a. Personally Identifiable Information;
   b. Individually Identifiable Health Information;

c. Non-public information related to the State's employees, customers, technology (including data bases, data processing and communications networking systems), schematics, specifications, and all information or materials derived therefrom or based thereon; or

d. Information designated as confidential in writing by the State.

G. CORE means the Comprehensive Outcome, Research, and Evaluation Reporting System. CORE is a web-based application that tracks participant-level diversion program and treatment court data for performance measurement and evaluation purposes.

H. CORE User means anyone with access to the CORE Reporting System, regardless of role. This could be an actual or contracted employee authorized to access the CORE Reporting System in some capacity.

I. CORE User Agreement means an agreement signed by a CORE User certifying that they (a) understand and agree to be bound by the laws regarding confidentiality of the records, information, and data contained in the CORE Reporting System; (b) agree not to disclose or use such records, information, and data contrary to law; and (c) agree to notify WI DOJ before any disclosure of CORE data.

J. Disclose means to release, transfer, provide, allow access to, or divulge in any other manner records, information, or data to anyone except the CORE user holding the records, information, and data.

K. Individually Identifiable Health Information means information that relates to the past, present, or future physical or mental health or condition of the individual, or that relates to the provision of health care in the past, present or future, and that is combined with or linked to any information that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

L. Participant means the person for whom a CORE user is entering data in the CORE Reporting System.

M. Personally Identifiable Information means the information described in Wisc. Stat. §943.201 (1) (b).

N. Program means a particular category of treatment court or diversion program within a site utilizing the CORE Reporting System.

O. Program User means a CORE Reporting System role describing an authorized user who enters and updates data in CORE for a particular program. There may be multiple program users per program per site.

P. Program Administrator User means a CORE Reporting System role describing an authorized user who oversees the entry and data quality at the program level for a particular program. Program administrator users are responsible for submitting user requests to site administrator users and monitoring user access and use of the system at the program level. Program admin users have full access to CORE to enter and update data and run reports. Only one program administrator user is authorized per program.

Q. Report User means a CORE Reporting System role describing an authorized user who can run assigned aggregate reports in CORE but cannot view or edit participant-level data.

R. Role refers to the capacity of a CORE user. Users may have multiple roles for various sites and programs within CORE.

S. Site means to either the county or tribe participating in the agreement to utilize the CORE Reporting System for one or more programs.

T. Site Administrator User means a CORE Reporting System role describing an authorized user who provides overall management of CORE access, entry, and data quality at the site level for one or more programs. Site admins are responsible for requesting, monitoring, and approving user access and use of the system for a site. Site admins have full access to CORE to enter and update data and run reports. Only one site administrator is authorized per site.

U. Use means the sharing, employment, application, utilization, examination, or analysis of records, information, or data.

V. User means an individual authorized to use the CORE Reporting System with one or more roles.

IV. PURPOSE

This MOU has been created so that employees, support personnel, contractors, and vendors of the site can participate in direct use of the Comprehensive Outcome, Research, and Evaluation (CORE) Reporting System. The CORE Reporting System is a web-based application being provided to counties and tribes for the collection, analysis, and reporting of participant-level data for treatment courts and diversion programs. CORE tracks participant data from referral to discharge for the purposes of evaluation and performance measurement. The system allows for on-going tracking of participant information such as demographics, mental health and substance abuse diagnosis, risk and needs assessment information, on-going progress updates including participation in treatment, drug or alcohol testing results, and incentives and sanctions administered, as well as review of program outputs and outcomes such as the following: program completion status, time in program, change in employment, education, and housing stability, reason for program termination, and related measures. In addition, the system will provide key information to assist in the evaluation of broader outcome and impact measures such as: incarceration days averted, post-program recidivism, comparison to traditional criminal justice outcomes, and cost/benefit analysis. The CORE Reporting System also has built-in reports for use by individual sites and programs.

This is a system designed for statewide use to collect participant data to improve the quality of treatment courts and diversion programs in Wisconsin. This system will provide individual sites and programs with a mechanism to track participant-level data for performance measurement and evaluation of program outcomes and impacts. The system will also provide WI DOJ access to

participant data from participating sites and programs that is needed to complete required evaluations outlined in Wis. Stat. § 165.95. Sites that have an alternative to incarceration grant under Wis. Stat. § 165.95 with WI DOJ are to submit their data through the CORE application on an on-going basis. Other sites may request to utilize the CORE Reporting System.

This agreement is for this stated purpose only, and any additional use or sharing of data entered into the CORE Reporting System in any form other than this purpose, or as otherwise required by law, is prohibited without the authorization of WI DOJ.

V. ACCESS

No individual may use the CORE Reporting System without the authorization of the site and the approval of WI DOJ. The site agrees to be responsible for CORE Reporting System use by all such individuals it authorizes, including its employees and contract and support personnel. If a site contracts with a noncriminal justice agency, or uses a noncriminal justice agency within the site to provide services required for the administration of criminal justice, and if that agency will have direct access to the CORE Reporting System, the site shall execute a Management Control Agreement between the site and the noncriminal justice agency. The Management Control Agreement shall be the same as or substantially similar to the form agreement attached to this MOU as attachment A. The site shall provide a copy of the agreement to WI DOJ for prior review and approval. The site shall not allow the noncriminal justice agency to have any access to the CORE Reporting System unless and until the site receives WI DOJ approval of the agreement. The agreement shall specifically authorize access to data, limit the use of data to purposes for which given, ensure the security and confidentiality of the data, and provide sanctions for violation thereof. It is the responsibility of the individual CORE User under this MOU to know the purposes for which any records, information, and data may be used and ensure that records, information, and data are used only for authorized purposes.

V.1 Roles

CORE will limit access to participant records or functions within the application in accordance with the user's role. There are multiple roles within CORE. The roles are as follows: BJIA Admin Users, Site Administrator Users, Program Admin Users, Program Users, and Report Users. WI DOJ reserves the right to update the security roles at any time. WI DOJ reserves the right to limitaccess to CORE Users at any time without notice.

Each CORE User shall be assigned one or more roles in CORE that provide access to different functions. Users may be assigned roles at one or more sites and for one or more programs. WI DOJ reserves the right to update the security roles and modify the system access for such roles at any time. Depending on roles assigned, CORE Users will have different levels of access to functions and respective participant records in CORE. A description of the role types is as follows:

Site Administrator – Provides overall management of CORE access, entry, and data quality at the local (county/tribe) level for one or more programs. Site Admins are responsible for requesting, monitoring, and approving user access and use of the system for the county/tribe. Site Admins have full access to CORE to enter and update data and run reports. Each site must designate one person as the site admin. Site Admins may also function as the Program Admin and/or Program User.

Program Admin – Oversees the entry and data quality at the program level for a particular program. Program Admins are responsible for submitting user requests to Site Admins and for monitoring user access and use of the system at the program level. Program Admins have full access to CORE to enter and update data and run reports. Each site must designate one program admin for each program it administers. Program Admins may also function as a Program User.

Program User – Enters and updates data in CORE for a particular program. There may be multiple program users per program per county/tribe.

Report User – Has the ability to run assigned aggregate reports in CORE, but cannot view or edit participant-level data.

V.2 Inter-Site Access

Each individual CORE User shall be assigned access to particular site(s) and program(s) in the system. No CORE Site or Program User may access any other program or site participant records unless authorized by the designated Site Administrator and approved by WI DOJ. WI DOJ will have access to all sites and programs for the purpose of monitoring data quality and conducting evaluation activities. WI DOJ will not disclose data to other sites without written permission from the Site Admin.

V.3 Access to identified participant information

Sites will have access to information that identifies individual participants based on the data recorded by the sites and dependent on user role access. Sites will not have access to identifiable participant information for data collected in the procedural fairness section of the CORE Reporting System, to maintain the confidentiality of participant responses. This data may be included in aggregate reports to the sites, but will not be provided to sites at the level of the individual respondent.

V.4 Passwords

WI DOJ's Bureau of Justice Information and Analysis (BJIA) will assign usernames and initial temporary passwords to CORE users after completion and approval of the User Agreement and the External User Authorization Form and will notify the new user of these identifiers. The initial

password will expire within 72 hours and must be reset to conform to CORE password requirements. Passwords will expire every 90 days. To comply with advanced authentication and security requirements, users must set up initial challenge questions and a four-digit PIN to be used when resetting passwords or locked accounts. User accounts will be locked after three failed login attempts with the challenge questions. Each individual user shall have a unique username and password that shall not be used by anyone except the individual user.

VI. SYSTEM CHANGES, SUPPORT, MAINTENANCE

The design of the system was completed by WI DOJ. WI DOJ will make changes as needed. Changes are identified through further discovery and implementation of the system.

WI DOJ will coordinate substantive changes (process flow, new screens, etc.) with the sites before any changes are made to the system. Minor changes such as modifications to dropdown lists or field formats will be made directly by WI DOJ and users will be informed of changes. WI DOJ shall have final authority with respect to all decisions regarding the design and configuration of the system.

WI DOJ will host the System and be responsible for primary support for the application.

VIII. CORE REPORTING SYSTEM RESPONSIBILITIES

Codes:

R Responsible for the activity
C Consulted about the activity
N/A Not Applicable

Entity	Responsibility	WI DOJ	Site
BCS	CORE is a web-based application. Provide required level of internet access to run the CORE application for WI DOJ users.	R	N/A
SITE IT	CORE is a web-based application. Provide required level of internet access to run the CORE application for any CORE Users outside of WI DOJ.	N/A	R
BCS	Provide secure storage of the CORE application, database, and data.	R	N/A
BCS	Modify the CORE application based on change requests submitted by BJIA.	R	N/A
BJIA	Review and approve change requests submitted by sites and coordinate changes with BCS.	R	N/A

Entity	Responsibility	WI DOJ	Site
BJIA	Create, update, and deactivate user accounts for CORE users based on validated user access requests from sites.	R	C
BJIA	Provide information to assist sites in determining the appropriate access level for users.	R	C
BJIA	Create, update, and deactivate user accounts for BJIA users after validating user access from supervisors.	R	N/A
BJIA	Complete user audits.	R	C
BJIA	Complete data audits as needed.	R	C
BCS	Assist BJIA in the completion of user and data audits as needed.	R	C
BCS	Complete security audits as needed.	R	C
BJIA	Answer business process questions and general application questions for CORE Users.	R	C
BJIA	Provide system support for CORE Users	R	C
BJIA	Perform application testing and sign off when BCS delivers updates or fixes prior to moving into production.	R	C
CORE Users	Request access to CORE through the designated site administrator for the appropriate site and program(s).	C	R
Site Admin	Approve a CORE Reporting System external user authorization request for each CORE user and submit to WI DOJ.	C	R
Site Admin	Request to deactivate any CORE user that should no longer have access to the CORE Reporting System.	C	R
Site Admin	Approve a CORE Reporting System external user authorization request for each program admin, program user, and report user and submit to WI DOJ.	C	R
Site Admin	Request to deactivate any program admin, program user, and report user that should no longer have access to the CORE Reporting System.	C	R

Entity	Responsibility	WI DOJ	Site
Site Admin	Responsible for security of CORE data for assigned sites and programs and reporting any potential security breaches.	C	R
Authorized Representative	Approve a CORE Reporting System external user authorization request for each site administrator admin user and submit to WI DOJ.	C	R
Authorized Representative	Request to deactivate any site administrator user that should no longer have access to the CORE Reporting System.	C	R
CORE Users	Responsible for appropriate handling of data based on legal requirements.	R	R
BJIA	Responsible for training WI DOJ staff in CORE application.	R	N/A
BJIA	Responsible for training site staff or providing training materials for the CORE application.	R	C

IX. INTERFACES AND CONVERSIONS

WI DOJ will not be responsible for any interfaces or conversions of data involving the CORE Reporting System or for any systems outside WI DOJ without prior WI DOJ approval and a separate project plan. WI DOJ will provide access to the CORE web service Application Program Interface (API) for sites providing data electronically for integration into the CORE Reporting System. No site shall create an interface into or out of the CORE Reporting System without prior WI DOJ approval. Any proposed interface or data conversion must provide adequate security to prevent unauthorized access of CORE data.

X. OPERATIONAL COSTS

Initially, WI DOJ will not bill the site for use or maintenance of the CORE Reporting System. If charges for use of the CORE Reporting System are subsequently imposed, any participating site may terminate this agreement upon providing 45 days advanced written notice to WI DOJ, unless required to report data to WI DOJ under Wis. Stat. §165.95.

XI. REQUIREMENTS FOR AND RESPONSIBILITIES OF SITES AND SITE EMPLOYEES, CONTRACTORS, ANDOTHER INDIVIDUALS UNDER THE SITES' CONTROL

Each Site shall:

a. Maintain a site administrator user to be responsible for communication, addressing site issues/questions, system changes, outages, etc. Site administrators shall contact WI DOJ with issues or site concerns.
b. Ensure that each user completes and submits the CORE Reporting System external user authorization request and user agreement prior to accessing the CORE Reporting System. A user who has completed and submitted an authorization request under a previous MOU does not need to complete and submit a new authorization request under this MOU.
c. Ensure that each user, including employees, contractors, and other individuals under the site's control, receives training prior to accessing the CORE Reporting System.
d. Immediately notify WI DOJ of any employees, contractors, and other individuals under its control or formerly under its control who are no longer authorized to access CORE. Immediate notification is critical given the web-based nature of the system.
e. Be responsible for all hardware, internet access, or interfaces necessary to access CORE. Ensure all workstations provide adequate security to prevent unauthorized access to CORE, including workstation timeout protocols and appropriate password safeguards.
f. Develop an internal process for immediately reporting to WI DOJ any potential breach or compromise of the security, confidentiality, or integrity of CORE or CORE information, and comply with or assist WI DOJ with any and all notification or remedial actions required by federal or state law, rule, or regulation. This includes any potential security breaches of any system interface to CORE or CORE data.
g. Provide WI DOJ access to any records, information, and data entered into CORE. This provision shall survive the termination, cancellation, or expiration of this MOU.
h. Use appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of records, information, and data obtained from CORE by its employees, contractors, and other individuals under its control consistent with law, regulations, and this MOU.
i. Ensure that informed consent is obtained by each program participant prior to the entry of Individually Identifiable Health Information including medical, mental health, and substance abuse information into CORE.
j. Provide employees, contractors, or other individuals under its control training on the various laws, regulations, and policies, including this MOU, which control access to and disclosure of records, information, and data contained in CORE.
    i. This training shall stress that all site employees, contractors, and other individuals under its control must have a valid, work-related reason to access or view any record, information, or data within CORE.
    ii. This training shall be provided to any such employee, contractor, or other

individual under its control prior to that individual's use of or access to CORE.

iii. Any employee, contractor or other individual must be trained no more than 120 days prior to being able to access CORE.

k. Identify a Site Administrator User. Additional users with one or more roles can be requested based on a defined need for access. There are multiple user roles within CORE. Sites are limited to only one CORE Site Administrator User and at a minimum a site.

l. Identify and request user access to CORE only for those employees having a defined business need. Ensure records, information, and data contained in CORE is used only for a valid work-related purpose.

m. Securely store any printed or electronic materials derived from CORE that contain confidential information and any records, information, or data obtained from the system to prevent unauthorized access. Securely destroy any material produced or derived from CORE.

n. Direct any public record requests for confidential information from CORE to WI DOJ.

o. Facilitate any requests for information by external evaluators to comply with the protocol developed by WI DOJ for the disclosure of information for evaluation purposes. Provide copies of evaluation contracts as requested by WI DOJ.

p. Prevent unauthorized disclosure of confidential information. Unauthorized disclosure, use or other release of records, information, or data derived from CORE may constitute a violation of law and could result in criminal and civil penalties and immediate termination of the Site's participation in this MOU and use of CORE.

q. Prevent unauthorized access to records, information, or data maintained in CORE. Unauthorized access by an individual user otherwise permitted access under this MOU constitutes a violation of the law and may result in criminal and civil penalties and immediate termination of the Site's participation in this MOU and use of CORE.

r. Ensure timely, accurate, and complete entry of data into CORE. The site can consult with WI DOJ to resolve questions as needed.

s. Ensure user has a unique username and password which shall not be shared. Use of a common or shared user ID is prohibited.

WI DOJ shall have the right to establish additional policies related to access to CORE which, upon written notice, shall immediately apply to each site, its employees, contractors, and other individuals under the site's control.

XII. REQUIREMENTS FOR AND RESPONSIBILITIES OF WI DOJ, ITS EMPLOYEES, CONTRACTORS, AND OTHER INDIVIDUALS UNDER ITS CONTROL

WI DOJ shall, in its sole discretion, use reasonable efforts to perform the following duties and responsibilities:

A. Provide information to sites regarding issues/questions, system changes, outages, and other

relevant matters.

B. Review, approve, and maintain a copy of the CORE Reporting System external user authorization request and user agreement prior to authorizing a user to access the CORE Reporting System.
C. Ensure that each user, including employees, contractors, and other individuals under WI DOJ's control, receives the appropriate training prior to accessing the CORE Reporting System.
D. Promptly deactivate a user upon notification from a site of any employees, contractors, and other individuals no longer needing access to CORE, including internal job transfer, resignation, discipline, or termination. The timeliness of this is imperative given the web-based nature of the system.
E. Maintain and support the CORE web application.
F. Develop an internal process for responding to any potential breach or compromise of the security, confidentiality, or integrity of CORE or CORE information, and complete any and all notification actions required by federal or state law, rule, or regulation. This includes any potential security breaches of any system interface to CORE or CORE data.
G. Use appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of records, information, and data obtained from CORE by its employees, contractors, and other individuals under its control consistent with law, regulations, policies, and this MOU.
H. Provide employees, contractors, or other individuals under its control training on the various laws, regulations, and policies, including this MOU, which control access to, and disclosure of records, information, and data contained in CORE.
    a. This training shall stress that all WI DOJ employees, contractors, and other individuals under its control must have a valid, work-related reason to access or view any record, information, or data within CORE.
    b. This training shall be provided to any such employee, contractor, or other individual under its control prior to that individual's use of or access to CORE.
    c. Any employee, contractor or other individual must be trained no more than 120 days prior to being able to access CORE.
I. Approve user access to CORE only for those employees having a defined business need.
J. Ensure records, information, and data contained in CORE is used only for a valid work-related purpose.
K. Securely store any printed or electronic materials derived from CORE that contain confidential information and any records, information, or data obtained from the system to prevent unauthorized access. Securely destroy any material produced or derived from CORE.
L. Direct any public record request for confidential information from CORE to WI DOJ Office of Open Government (OOG). The OOG will follow the established redaction and distribution procedure. Records, information, and data from CORE that contain confidential information shall not be re-disclosed to any person or agency contrary to law and without the written approval of WI DOJ.
M. Coordinate requests for aggregate CORE data with WI DOJ's OOG.

N. Prevent unauthorized disclosure of confidential information. Unauthorized disclosure, use or other release of records, information, or data derived from CORE may constitute a violation of law and could result in criminal and civil penalties.
O. Prevent unauthorized access to records, information, or data maintained in CORE. Unauthorized access by an individual user otherwise permitted access under this MOU constitutes a violation of the law and may result in criminal and civil penalties.
P. Ensure disclosure of confidential information from CORE will only occur back to the site.
Q. Prevent re-disclosure of information from CORE except as authorized by applicable state and federal laws.
R. Develop a protocol for external evaluators to request data from CORE that complies with applicable state and federal laws.
S. Develop reports to facilitate site use of the information contained in CORE and to support performance measurement and evaluation activities, as well as to communicate data quality questions with sites to help ensure timely, accurate, and complete entry of data into CORE.

XIII. PROTECTION OF CONFIDENTIALITY AND UNAUTHORIZED DISCLOSURE OR USE

The site, for itself, its employees, other individuals under control of the site, and WI DOJ agree that all personnel with access to records, information, and data obtained from the CORE Reporting System covered by this MOU must comply with all state and federal laws regarding privacy and confidentiality of said records, information, and data and to policies and procedures regarding privacy and confidentiality as set forth by the site and WI DOJ. As CORE records may contain confidential information pertaining to an individual's criminal background, alcohol and drug use, mental health records, health care records, and personally identifiable information, users must comply with state and federal laws and regulations pertaining to the confidentiality of such data. Each site shall implement all procedures necessary to protect the CORE Reporting System information from any unauthorized use. These procedures include, but are not limited to, the requirements in this document.

Consistent with Wisconsin and federal law, the site, its employees, and other individuals under the control of the site, including contractors, shall not use or disclose any records, information, or data obtained from CORE contrary to federal or state laws, or without prior written approval from WI DOJ in accordance with this MOU.

Any presentations, reports, and research articles (including drafts of any of these) based on data covered by this agreement may present data in aggregate form only. No aggregate information that would enable the direct or indirect identification of an individual may be published without prior written permission from WI DOJ.

Users accessing CORE must have appropriate WI DOJ authorization and a valid, work-related reason to access or review any information in the system. CORE use is solely for authorized business purposes. Any personal use of the system will result in a loss of access to the system and further legal and administrative action. Access to or dissemination of information contained in CORE must be in compliance with the following or any other applicable laws:

- AODA, State Alcohol, Drug Abuse, Developmental Disabilities or Mental Health records
  - 42 C.F.R. § 2
  - Wis. Stat. § 51.30
- Medical or Health Care records
  - 45 C.F.R. §§ 160, 164
  - Wis. Stat. § 146.82
- Criminal History information
  - 28 C.F.R. § 20
- Juvenile Records
  - Wis Stat. § 48.396
  - Wis. Stat. § 48.78
  - Wis. Stat. § 938.396
  - Wis. Stat. § 938.78

Each user requiring access to CORE must complete the CORE Reporting System user agreement and the CORE Reporting System external user authorization request, which shall be kept on file by WI DOJ for each user that has access to CORE.

CORE requires identifiers in the system for each participant, which are necessary to allow for linking to other data sources for evaluation purposes. The state identification number (SID) will be required for all new participant records. If no SID exists for a participant, other key identifiers will be required, such as the Department of Corrections (DOC) number, Social Security Number (SSN) at least last 4 digits, or Human Services Reporting System (HSRS) number. The site agrees not to insert any numbers into the key identifier fields other than valid identifier numbers or a value identified by WI DOJ to represent an unknown value. This restriction ensures data integrity within CORE and other Wisconsin criminal justice information systems and maintenance of accurate identifier information for participants.

XIV. WI DOJ ACCESS TO SITE RECORDS TO CONDUCT QUALITY CHECK

The site shall provide WI DOJ access to any of its records, information, and data contained in the CORE Reporting System for the purposes of conducting audits to ensure compliance with this MOU and with the law. Likewise, WI DOJ will work with the site to provide standard reports that will assist in identifying data quality issues such as duplicate participant records, unauthorized temporary SIDs, and other such matters.

WI DOJ shall, at any time during normal business hours and upon reasonable notice, have access to and the right to examine, audit, excerpt, transcribe, and copy, on the site's premises, any of the site's records and computer data storage media involving transactions directly pertinent to this MOU. If the material is on computer data storage media, the site shall provide copies of the data storage media or a computer printout of the records upon WI DOJ request. Charges for copies of books, documents, papers, records, computer data storage media or computer printouts provided by the site shall not exceed the actual cost to the site. This provision shall survive the termination, cancellation, or expiration of this MOU.

XV. SECURITY VIOLATIONS

The site shall inform WI DOJ within 24 hours if the site becomes aware of any threatened or actual use or disclosure of any information not specifically authorized by this agreement. At all times, the site shall exercise due diligence to assure the detection of any such unauthorized use or disclosure. The site shall inform WI DOJ if any information is lost or cannot be accounted for, within 24 hours from the site's knowledge of such use, disclosure, or loss. Notice for both incidents shall identify the person affected and the information disclosed. The site shall take all of the following steps, as required by WI DOJ:

1. Take immediate steps to mitigate any harmful effects of any unauthorized use, disclosure, or loss. The site shall cooperate with WI DOJ's efforts to seek appropriate injunctive relief or otherwise prevent or curtail any threatened or actual breach, or to recover confidential information, including complying with a reasonable corrective plan;
2. Notify the affected individuals by mail or by a method reasonably calculated to provide actual notice. At a minimum, the notice shall indicate that the site knows of the unauthorized acquisition of personal information pertaining to the affected individual.;
3. Conduct an investigation into the matter as directed by WI DOJ, providing results and updated information as it becomes available to WI DOJ; and
4. Provide other services or assurances to mitigate or prevent further damage resulting or potentially resulting from the breach.

The site shall also immediately suspend access of any CORE User involved in a potential security violation pending the results of the investigation.

WI DOJ may, at its sole discretion, terminate the site's participation under this agreement as a consequence of any such violations or potential violations. Upon notification to the site, WI DOJ shall have the right to conduct an investigation of the potential security violation. WI DOJ may suspend or terminate access to CORE. WI DOJ may reinstate the site's access to CORE after the site provides assurances satisfying WI DOJ that the site has taken appropriate actions to prevent

a recurrence.

The site acknowledges that the unauthorized use, disclosure, or loss of information may cause immediate and irreparable injury to the individual(s) whose information is disclosed and to WI DOJ, which injury will not be compensable by money damages and for which there is not an adequate remedy available at law. Accordingly, the parties agree that WI DOJ, on its own behalf or on behalf of the affected individual(s), shall be entitled to any injunctive or other equitable relief required to prevent, curtail, or mitigate damage from, any such breach, threatened or actual.

XVI. TERMINATION OF THIS MOU

WI DOJ may unilaterally terminate this MOU for any violations of law, regulations, or policies including those set forth in this MOU regarding the use of the CORE Reporting System by the site, its agencies, its employees, its contractors, or other individuals under its control.

This MOU may also be terminated by mutual written agreement of WI DOJ and an authorized representative of the site. The party wishing to terminate this MOU must provide forty-five (45) days written notice to the other party stating the desire to terminate and the reasons. The responding party must reply in writing within thirty (30) days indicating whether the termination request will be approved or denied, and the reasons. Both authorized parties agree to negotiate if an agreement cannot be immediately reached.

Upon termination of this agreement, any data entered by site employees in CORE remains the property of WI DOJ. A copy of the data for the applicable site and programs(s) can be securely provided to the site upon agreement of both parties.

All or part of this MOU may be amended at any time by written amendment approved by the signatories identified in Section XVIII of this MOU or their successors.

This MOU is subject to applicable law, which is subject to change. If applicable law changes, this MOU will be deemed to be immediately modified in accordance with each such change, without notice or written amendment.

Each party shall notify the other immediately upon learning of any law change which may affect the terms of this MOU. The parties further agree to meet within sixty (60) days from receipt of such notice in a good faith attempt to negotiate an amendment which will ensure the legality and enforceability of this MOU, if necessary.

The confidentiality and disclosure requirements of this agreement survive the termination, for whatever reason, of the agreement itself, subject to applicable state and federal statutes and administrative rules.

XVII. CONTACTS FOR ADMINISTRATION OF THIS MOU

For the Site:

Sauk County

Site Name

Site Mailing Address, Line 1

Site Mailing Address, Line 2 (optional)

510 Broadway Street, Baraboo, WI 53913

Site Mailing Address, City, State, Zip Code

Amanda Hanson

Site Contact Person's Name

amanda.hanson@saukcountywi.gov

Site Contact Person's Email Address

(608) 355-4884

Site Contact Person's Phone Number

For WI DOJ:

Bureau of Justice Information and Analysis (BJIA)
Wisconsin Department of Justice – Division of Law Enforcement Services
17 West Main Street
Madison, Wisconsin 53703-7857

Phone: (608) 266-0605
Email: core@doj.state.wi.us

XVIII. AUTHORIZATION

The duly authorized undersigned representatives of DOJ and Agency hereby agree to the policies, procedures, terms, and requirements set forth in this MOU. Each signatory guarantees that all of signatory's staff, contractors/subcontractors, limited term staff and unpaid personnel will abide by all confidentiality restrictions set forth in this MOU.

Agreed and accepted:

Eric J. Wilson
Deputy Attorney General
Wisconsin Department of Justice

Date Signed

Signature*

Brent Miller

Signatory's Name

County Administrator

Signatory's Title

Sauk County Justice, Diversion, and Support

Department/Office/Agency

Date Signed

*This electronic signature is legally enforceable under the Wisconsin Uniform Electronic Transactions Act, as well as other applicable state and federal laws.