DUPAGE COUNTY

DATA SECURITY EXHIBIT

This Data Security Exhibit ("Exhibit") is incorporated into and made a part of the Agreement between the County of DuPage ("County") and the Vendor identified in the Agreement ("Vendor"). Capitalized terms not defined herein shall have the meanings ascribed to them in the Agreement.

Section 1. Purpose and Scope

The purpose of this Exhibit is to establish the data security, records management, accessibility, and information governance requirements that apply to all Vendor services, products, and systems provided to or on behalf of the County. This Exhibit applies to all data created, received, maintained, processed, transmitted, or stored by Vendor in connection with the performance of Services under the Agreement.

Vendor acknowledges that the County is a unit of local government in the State of Illinois and is subject to federal, state, and local laws and regulations governing data security, records management, accessibility, and privacy. Vendor shall comply with all such applicable laws and regulations, as well as the specific requirements set forth in this Exhibit.

This Exhibit applies only to County Data that is actually processed, stored, or transmitted by Vendor as part of the Solution. Vendor shall not be responsible for data types (including CJI or PHI) that are not intentionally collected or required for the performance of Services. County shall not intentionally and knowingly upload or transmit CJI or PHI into the Solution without Vendor's prior written approval.

Where the Services involve access to Criminal Justice Information (CJI) or Protected Health Information (PHI), the applicable provisions of Sections 10 and 11 of this Exhibit shall apply *in addition to* all other requirements set forth herein. In the event of a conflict between the general provisions of this Exhibit and the requirements of Sections 10 or 11, the more restrictive requirement shall govern.

Section 2. Definitions

- **"Business Associate"** has the meaning set forth in the HIPAA Rules at 45 CFR 160.103, and refers to any person or entity that performs certain functions or activities involving the use or disclosure of PHI on behalf of, or provides services to, a Covered Entity.
- **"CJI" or "Criminal Justice Information"** means all data provided and collected by the FBI's Criminal Justice Information Services Division, including but not limited to biometric data, identity history data, person data, property data, and

case/incident history data, as well as Criminal History Record Information (CHRI). CJI is subject to the FBI CJIS Security Policy, as amended from time to time.

- **"CJIS Security Addendum"** means the uniform addendum approved by the U.S. Attorney General that extends the requirements of the CJIS Security Policy to private contractors, vendors, and third parties who have access to CJI.
- **"CJIS Security Policy"** means the FBI Criminal Justice Information Services Security Policy, currently Version 6.0 (December 2024), as may be updated or superseded from time to time, which establishes the minimum-security requirements for the access to, and protection of, CJI.
- **"Confidential Information"** means any data, records, documents, or other information, in any form, that is not generally known to the public and is created, collected, received, maintained, processed, transmitted, or stored by Vendor in connection with the Agreement, including but not limited to: PII, PHI, CJI, financial records, law enforcement records, employee data, technical data and specifications, and any other information designated as confidential by the County.
- **"County Data"** means all data and records that are the property of the County or that are created, collected, or processed on behalf of the County, regardless of the media or format in which such data is maintained.
- **"Covered Entity"** has the meaning set forth in the HIPAA Rules at 45 CFR 160.103.
- **"HIPAA"** means the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH Act, Title XIII of the American Recovery and Reinvestment Act of 2009), and all regulations promulgated thereunder, including the Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164), the Security Rule (45 CFR Part 160 and Subparts A and C of Part 164), and the Breach Notification Rule (45 CFR Part 160 and Subparts A and D of Part 164) (collectively, the “HIPAA Rules”).
- **"PHI" or "Protected Health Information"** has the meaning set forth in the HIPAA Rules at 45 CFR 160.103 and includes individually identifiable health information transmitted or maintained in any form or medium. “ePHI” refers to PHI that is transmitted or maintained in electronic media.
- **"PII" or "Personally Identifiable Information"** means information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.
- **"Public Record"** has the meaning ascribed under the Illinois Local Records Act (50 ILCS 205/3), and includes any book, paper, map, photograph, digitized electronic material, or other official documentary material, regardless of physical form or characteristics, made, produced, executed, or received by any agency or officer pursuant to law or in connection with the transaction of public business.

- **"Solution"** means the system, platform, software, application, or service provided by Vendor to the County under the Agreement, including all components, interfaces, and associated documentation.
- **"WCAG"** means the Web Content Accessibility Guidelines published by the World Wide Web Consortium (W3C).

Section 3. System and Architecture Requirements

Vendor systems and capabilities must meet the following minimum requirements:

- The application architecture shall be built with security as a foundational principle, using current industry frameworks and standards, such as NIST Cybersecurity Framework, NIST SP 800-53, or ISO/IEC 27001.
- The environment must be redundant, with no single points of failure, and have the capacity to handle the County's operational demands and the capability to recover from data loss or corruption.
- The Solution must integrate with the County's designated log management platform or Vendor shall provide access to standard system logs and reports. Custom integration with County log management systems may be provided as an optional service subject to feasibility and additional fees.and maintain logs of activities, status, and functional state of the Solution.
- The Solution must leverage the County's system of record for identity and access management, supporting SAML-based single sign-on and other County-approved authentication protocols (OAuth, ADFS).
- The Solution must support open data exchange for all data within the proposed system using SFTP, third-party APIs, or an open API for data exchanges, aligned with the County's administrative data management programs.
- The Solution must enable reporting and analytics (BI) for all data provided or generated applicable only to the extent such functionality is included in the Solution as described in the Agreement.
- The Solution must support scheduled, automated imports and exports of data.
- The Solution must include quality controls for data management within the user interface and within data synchronization routines.
- Vendor must employ named experts to work in collaboration with County IT and business experts.

Note: Where the Solution processes CJI, additional architecture requirements as set forth in Section 10 of this Exhibit shall also apply, including FIPS 140-validated encryption modules and alignment with NIST SP 800-53 Rev. 5. Where the Solution processes PHI, additional requirements as set forth in Section 11 shall also apply.

Section 4. Data Integrations and Data Accessibility

4.1 Data Integrations

The Solution shall support both ad hoc and automated import, export, and update of all necessary data for the in-scope systems, at appropriate frequencies, including near-real-time.

4.2 Data Accessibility

Vendor shall support both ad hoc and automated extract of all data from the Solution at appropriate frequencies, or as needed to support County processes.

4.3 Data Validation

Integration of multiple datasets can be fraught with difficulty, including inconsistent fields, missing datasets, and conflicting information. The Solution shall include rules to ensure referential integrity between datasets:

- Ensure that primary keys in one dataset are unique, including compound primary keys.
- Ensure that foreign keys in one file match the primary keys in another file.
- Validate that all other fields are well formed and cleaned as required.

The Vendor shall also provide the following data quality mechanisms:

- Automatic quarantining of data to ensure that invalid data is not ingested. Even if only part of a file is invalid, the invalid data shall be removed and the remainder quarantined.
- Email alerts when data issues are identified so, they can be quickly escalated when jobs are not synchronized.

4.4 Data Conversion and Validation

Vendor must provide qualified personnel to partner with the County's Enterprise Data and Identity and Access Management teams to document proper conversion mapping and perform test validation for all bi-directional data exchanges and automations.

4.5 Third-Party Integrations

For any third-party integration, Vendor shall document the purpose, data exchanges, utility of integration, method of integration, geography of operations, and the name of the third party. All third-party integrations require formal written approval from County IT prior to implementation.

Section 5. Data Management and Protection

5.1 Data Management

- Vendor shall not copy any County Data to any media, including hard drives, flash drives, or other electronic devices, other than as expressly approved in writing by the County.
- Vendor shall return or destroy all Confidential Information received from the County or created or received by Vendor on behalf of the County, upon request from the County.
- In the event that returning or destroying Confidential Information is infeasible, Vendor shall notify the County of the conditions that make return or destruction infeasible. Such determination must be approved by the County, and Vendor shall extend protections, and limit further uses and disclosures of such information.
- Vendor shall return all County Data in an electronic format via a secure service, such as SFTP, API, or secure online shared storage facility.
- Security practices regarding secure application development and permissioning must be documented and approved by the County.

5.2 Encryption and Data in Transit

The Solution shall support the latest encryption standards and TLS protocols for data in motion and at rest for all Confidential Information and PII. Where CJI is involved, encryption shall meet the requirements of FIPS 140 validation as specified in Section 10. Where ePHI is involved, encryption shall comply with HIPAA Security Rule requirements as specified in Section 11.

5.3 Data Backup and Recovery

County Data shall be protected with current backup technologies and backed up daily (at least every 24 hours, unless otherwise agreed), with retention of no less than thirty (30) days, and for the duration of the Agreement. Backup and recovery capabilities shall exist within both production and disaster recovery environments. All County Data shall be hosted and protected within the continental United States.

5.4 Audit History

The Solution shall maintain a complete history of all data, including user identification and timestamps for data creation, updates, and deletions, to support a complete audit trail for the duration of the Agreement. This includes persistence of deleted data (“soft deletes”) for all key entities as determined by County requirements. Reporting on audit history shall be efficient and shall preferably include out-of-the-box reports summarizing data changes. Vendor shall provide the County with a data model for logs and a method for the County to access this information.

Section 6. Identity and Access Management

- The Solution must comply with the County’s Security and Access Control policies.

- Any third party, subcontractor, employee, or agent to whom access to County Data or information systems is granted must agree to the same restrictions, standards, and conditions that apply under this Agreement, and such access must be approved by the County.
- All parties with access to County Data shall implement reasonable and appropriate safeguards to ensure the confidentiality, integrity, and availability of the data and information systems.
- Vendor shall maintain access controls, security policies, and incident response plans that comply with NIST, ISO/IEC 27001, and current County security policies.
- Vendor shall report to the County's Chief Information within twenty-four (24) hours of discovery of any security incident . that materially compromises the security, confidentiality, or availability of the Solution as it relates to County Data
- Vendor shall maintain audit event logs according to County policy and provide this information to the County upon request.
- Vendor shall develop and implement policies and procedures describing how users are to protect against intrusion, tampering, viruses, and other threats.
- The Solution shall support authentication integration with Active Directory, including user account and password requirements compatible with the latest version of SAML protocol or other County-approved SSO service platforms. Where required for solution integration, County shall provide necessary support including meeting with Vendor and implementation. County is responsible for any costs arising from this integration including necessary licensing costs from County-approved SSO platform.

Note: Where CJI is involved, Vendor personnel must also satisfy the background check, security awareness training, and multifactor authentication requirements set forth in Section 10. Where PHI is involved, access must be limited to the minimum necessary standard as required by Section 11.

Section 7. Portability and Disentanglement

7.1 Data Portability

The County must be able to retrieve its data and applications from the Solution and migrate them into different County environments or directly to a successor solution at the expiration or termination of the Agreement. If the Solution uses proprietary software or formats to store County Data, Vendor shall transform the data into a format suitable for County consumption at no additional cost. The County may also need to retrieve data to respond to Freedom of Information Act ("FOIA") requests or to fulfill other legal obligations. To that end, the data format shall be susceptible to digital redaction such that a portion or all the data may be redacted digitally prior to production of the data.

7.2 Disentanglement Plan

Vendor shall work with the County to establish a Disentanglement Plan as a deliverable, to be executed at the end of the Agreement term (including any renewals). The Disentanglement Plan shall include:

- Transfer of all County-generated information to the County in a format specified by the County.
- Deletion of all County information from Vendor's systems after the County receives and validates the data, including working copies, backup copies, and data in development or staging environments.
- Certification in writing by Vendor that all County Data has been transferred and/or destroyed in accordance with the County's direction.

Section 8. Records Management and the Illinois Local Records Act

All records created, received, maintained, or transmitted by Vendor in connection with the performance of Services under this Agreement that constitute Public Records of the County are subject to the Illinois Local Records Act (50 ILCS 205) ("ILRA"). Vendor acknowledges that the County is legally obligated to preserve, manage, and dispose of Public Records in accordance with the ILRA and retention schedules approved by the Local Records Commission.

8.1 Record Preservation and Retention

- Vendor shall not destroy, alter, deface, remove, or conceal any Public Record of the County, whether in physical or electronic form, except as expressly authorized in writing by the County and in accordance with an approved retention schedule.
- Vendor shall maintain all records generated, collected, or processed on behalf of the County for the retention periods specified in the County's applicable retention schedules, or as otherwise directed by the County. In the absence of a specific retention schedule, Vendor shall retain all such records for a minimum of seven (7) years following the expiration or termination of this Agreement, unless a longer period is required by law.
- Vendor shall store and manage County records in a manner that ensures their integrity, authenticity, reliability, and usability for the full duration of the applicable retention period.

8.2 Electronic Records Standards

- Any electronic records system used by Vendor to create, store, or manage County records must reproduce original records accurately and legibly in all details and must not permit unauthorized additions, deletions, or changes to original document images.
- Electronic records must be retained in a trustworthy manner so that the records and the information contained therein are always accessible and usable for subsequent reference during the applicable retention period.

- Vendor shall ensure that electronic records are maintained in non-proprietary or widely supported formats or shall provide the County with the tools and documentation necessary to access and use the records independently of Vendor's systems.

8.3 Disposition and Disposal

- Vendor shall not dispose of or destroy any County records without the prior written authorization of the County and, where applicable, approval from the Local Records Commission through a Records Disposal Certificate.
- Upon request, Vendor shall cooperate with the County in preparing Applications for Authority to Dispose of Local Records and Records Disposal Certificates as required under the ILRA.
- Upon expiration or termination of this Agreement, Vendor shall transfer all County records to the County in an electronic format specified by the County and shall certify in writing the complete transfer or destruction of all copies, including backup and archival copies, in accordance with the County's direction.

8.4 Freedom of Information Act Support

- Vendor acknowledges that County records in Vendor's possession may be subject to disclosure under the Illinois Freedom of Information Act (5 ILCS 140). Vendor shall provide reasonable assistance to the County in responding to FOIA requests, including producing responsive records in the format requested, within the timeframes required by law.
- Vendor shall not independently respond to any FOIA, or other public records request directed at County Data without prior written authorization from the County.

8.5 Essential Records Protection

Vendor shall cooperate with the County's efforts to identify, protect, and preserve essential records necessary for the continuity of governmental functions in the event of an emergency, consistent with the ILRA's requirements for essential records programs.

8.6 Penalties

Vendor acknowledges that the knowing and unauthorized alteration, destruction, defacement, removal, or concealment of Public Records is a Class 4 felony under Illinois law (720 ILCS 5/32-8). Vendor shall ensure that all employees, agents, and subcontractors who handle County records are informed of their obligations under the ILRA and this Agreement.

Section 9. Digital Accessibility – ADA Title II Compliance

The County is subject to Title II of the Americans with Disabilities Act (42 U.S.C. § 12131 et seq.) and the Department of Justice's final rule on accessibility of web information and services of state and local government entities, published April 24, 2024

(28 CFR Part 35). This rule requires the County to ensure that its web content and mobile applications conform to WCAG Version 2.1, Level AA. To the extent that the Services, Solution, or any deliverables under this Agreement include web-based content, applications, portals, or mobile applications made available to the public or used by the County in the delivery of its services, programs, or activities, Vendor shall comply with the following:

9.1 WCAG Conformance

- All web content, web applications, portals, dashboards, public-facing interfaces, and mobile applications provided, hosted, or maintained by Vendor shall conform to WCAG 2.1, Level AA (encompassing both Level A and Level AA success criteria) at the time of delivery.
- The parties acknowledge that ongoing conformance to WCAG 2.1, Level AA is dependent on a variety of factors outside of Vendor's control, including but not limited to content updates, document uploads, configuration changes, and third-party scripts or integrations implemented by or at the direction of the County.
- Accordingly, continued conformance following go-live is not guaranteed and requires ongoing monitoring, testing, and remediation. Vendor offers accessibility scanning and remediation services designed to support ongoing compliance, which are not included in the base Services unless expressly set forth in the Agreement.Conformance shall be maintained whenever updates, upgrades, patches, or new features are deployed.
- Vendor shall, at contract execution and annually thereafter as well as upon request, provide a current Voluntary Product Accessibility Template (VPAT) or equivalent accessibility conformance report documenting the Solution's conformance with WCAG 2.1, Level AA.

9.2 Scope of Accessibility Obligations

- Accessibility compliance is a shared responsibility between Vendor and the County. Vendor's accessibility obligations extend to all components of the Solution used by the County to deliver services, programs, or activities to the public, including but not limited to online forms, document viewers, interactive tools, multimedia content, notification systems, and self-service portals. The County is responsible for ensuring the accessibility of all content, documents, media, and configurations that it creates, uploads, modifies, or manages within the Solution.
- Where the Solution generates or outputs electronic documents that will be made available to the public, such documents shall conform to applicable accessibility standards, including PDF/UA (ISO 14289-1) for PDF documents. Other electronic documents made available to the public (including .docx, .xlsx, and .pptx formats) shall conform to applicable accessibility standards equivalent to WCAG 2.1, Level AA provided these documents have been created by the County to conform to these standards originally. Alternatively, Vendor may offer automated

tools such as a PDF-to-HTML conversion tool, which provides WCAG conforming alternatives to these formats.

- All multimedia content embedded in or delivered through the Solution shall include captions for prerecorded and live audio content, and audio descriptions for prerecorded video content, as required by WCAG 2.1, Level AA.

9.3 Testing and Remediation

- Vendor shall perform accessibility testing using a combination of automated tools and manual testing methods (including testing with assistive technologies such as screen readers) prior to initial deployment and following any updates; including any release, patch, feature addition, or configuration change that affects public-facing interfaces or document output.
- Vendor shall remediate any accessibility deficiencies, excluding County-managed content, configuration changes, or third-party components identified through testing, user reports, or County audits within thirty (30) calendar days of notification, or within such other timeframe as mutually agreed for complex remediation efforts.
- Accessibility issues arising from County-managed content, configuration changes, or third-party components shall be the responsibility of the County unless Vendor's optional accessibility services are engaged. Vendor shall provide documentation of accessibility testing results and remediation activities upon request.

9.4 Third-Party Components

- Vendor shall not be responsible for accessibility issues arising from third-party components, plug-ins, widgets, scripts, or embedded content that are not developed or controlled by Vendor. Vendor shall make commercially reasonable efforts to inform the County of known accessibility considerations associated with third-party integrations where applicable. As a courtesy, Vendor will make itself available, upon request, to provide general, consultative guidance to the County regarding accessibility considerations and best practices when evaluating or implementing third-party components. Such guidance is advisory in nature and does not constitute a guarantee of accessibility compliance for third-party components or services. Vendor shall include accessibility conformance requirements where applicable in any agreements with subcontractors or third parties who contribute to the Solution.

9.5 Contractor Responsibility

Under the DOJ's final rule, state and local governments that contract with other entities to provide public services remain responsible for ensuring that their contractors comply with Title II. Vendor acknowledges this obligation and agrees to cooperate fully with the County to ensure the Solution meets all applicable accessibility requirements.The parties acknowledge that the DOJs final rule or Title II of the ADA does allow for exceptions. Parties agree to work in good faith to avoid invoking these exceptions

where a commercially viable solution is reasonable. Any request by Vendor to invoke such an exception must be submitted in writing, with supporting documentation sufficient for the County to evaluate the claim and shall not take effect unless and until the County provides written approval. Failure to achieve or maintain a high level of WCAG 2.1, Level AA conformance may constitute a breach of this Agreement, subject to the cure and default provisions of the Agreement.

9.6 Ongoing Compliance

- The parties acknowledge that accessibility compliance requires ongoing monitoring and remediation due to the dynamic nature of web content and evolving standards.
- Vendor shall designate a qualified individual as an accessibility point of contact to coordinate with the County on accessibility matters.
- Vendor shall ensure that the Solution includes or supports an accessible mechanism by which users may report accessibility barriers or request accommodations, and shall ensure that such mechanism itself conforms to WCAG 2.1, Level AA.
- Vendor shall monitor changes to applicable accessibility standards and regulations and shall notify the County of any anticipated impacts to the Solution's conformance.
- Vendor shall provide training documentation or guidance to County staff, as reasonably requested, to support the creation and maintenance of accessible content within the Solution.
- Vendor offers accessibility scanning and remediation services designed to support ongoing compliance, including identification and correction of accessibility issues affecting both platform components and rendered content. Such services are not included in the base Services unless expressly set forth in the Agreement.

Section 10. Criminal Justice Information Services (CJIS) Compliance

Applicability. This Section applies when the Services, Solution, or any component thereof involves the creation, access, receipt, storage, processing, transmission, or destruction of CJI on behalf of the County and is explicitly agreed to as a deliverable service in a written agreement or amendment signed by both parites. Where this Section applies, its requirements are in addition to all other requirements of this Exhibit and shall be deemed incorporated into every aspect of Vendor's obligations under the Agreement.

10.1 CJIS Security Policy Compliance

- Vendor shall comply with the FBI CJIS Security Policy, as amended from time to time (currently Version 6.0, December 2024), and all applicable federal and State of Illinois regulations governing the access to and protection of CJI.

- Vendor shall align its security controls with NIST SP 800-53 Rev. 5, consistent with the CJIS Security Policy's control-based framework.
- Vendor shall monitor updates to the CJIS Security Policy and implement required changes within the timeframes specified by the FBI CJIS Division or the Illinois State Police, as the CJIS Systems Agency (CSA) for the State of Illinois.

10.2 CJIS Security Addendum

- Vendor and all Vendor personnel who will have access to CJI shall execute the CJIS Security Addendum prior to being granted access to any CJI or systems that process CJI.
- Vendor shall ensure that all subcontractors, agents, and third parties who may have access to CJI also execute the CJIS Security Addendum and comply with all applicable CJIS requirements.
- Vendor shall maintain executed copies of the CJIS Security Addendum and make them available to the County upon request.

10.3 Personnel Security

- All Vendor personnel who will have access to CJI, or to systems that process or store CJI, shall undergo a state and national fingerprint-based background check prior to being granted access. Background checks shall be adjudicated by the County or its designee in accordance with CJIS Security Policy requirements.
- Vendor personnel who do not pass the required background check shall not be granted access to CJI or to any County systems that process CJI and shall be immediately removed from any CJI-related duties.
- All Vendor personnel with access to CJI shall complete CJIS Security Awareness Training within six (6) months of initial assignment and annually thereafter, as required by the CJIS Security Policy.

10.4 Access Controls and Authentication

- Access to CJI shall be restricted to authorized personnel on a need-to-know, need-to-use basis, based on the principle of least privilege.
- Vendor shall implement and enforce multifactor authentication (MFA) for all users accessing CJI or systems that contain CJI, using phishing-resistant MFA methods where technically feasible, consistent with CJIS Security Policy Version 6.0 requirements.
- Vendor shall implement role-based access controls and maintain a current list of all personnel authorized to access CJI, which shall be provided to the County upon request.
- Vendor shall promptly revoke access to CJI for any personnel who no longer require access, including upon termination, reassignment, or change of role.

10.5 Encryption

- CJI shall be encrypted in transit and at rest using cryptographic modules validated under FIPS 140 (currently FIPS 140-3), as required by the CJIS Security Policy.
- Encryption key management practices shall comply with CJIS Security Policy requirements and industry best practices.

10.6 Audit and Monitoring

- Vendor shall maintain detailed audit logs of all access to, and activity involving, CJI, including user identification, date and time of access, type of activity, and success or failure of access attempts.
- Audit logs shall be retained for a minimum period consistent with the CJIS Security Policy and shall be made available to the County, the Illinois State Police (as CSA), or FBI CJIS Division auditors upon request.
- Vendor shall support and cooperate with CJIS compliance audits conducted by the County, the Illinois State Police, or the FBI CJIS Division, including providing access to systems, facilities, records, and personnel.

10.7 Incident Response

- Vendor shall report any security incident involving or potentially involving CJI to the County's Chief Information Officer and to the Illinois State Police CJIS Systems Officer (CSO) within one (1) hour of discovery.
- Vendor shall maintain a written incident response plan that addresses CJI-specific incidents and shall provide a copy to the County upon request.
- Vendor shall cooperate fully with any investigation conducted by the County, the Illinois State Police, or the FBI CJIS Division related to a security incident involving CJI.

10.8 Physical Security

Vendor shall implement physical security controls sufficient to protect any facility, equipment, or media where CJI is stored, processed, or accessed, consistent with the CJIS Security Policy. This includes, but is not limited to, controlled facility access, visitor logs, and secure disposal of physical media containing CJI.

10.9 Cloud Services

If the Solution utilizes cloud-based infrastructure for the storage, processing, or transmission of CJI, the cloud service provider must meet CJIS Security Policy requirements and maintain an executed CJIS Security Addendum. The County retains the right to approve or reject the use of any cloud service provider for CJI-related services.

Section 11. HIPAA Compliance and Business Associate Obligations

Applicability. This Section applies when the Services, Solution, or any component thereof involves the creation, receipt, maintenance, transmission, or storage of PHI on behalf of the County or any County department that operates as a Covered Entity or hybrid entity under HIPAA. Where this Section applies, Vendor acknowledges that it is acting as a Business Associate of the County, and the terms of this Section shall constitute the Business Associate Agreement ("BAA") required under 45 CFR 164.502(e) and 164.504(e).

11.1 Permitted Uses and Disclosures

- Vendor shall not use or disclose PHI other than as permitted or required by this Agreement or as required by law.
- Vendor shall use PHI only for the purpose of performing the Services described in the Agreement and shall not use or disclose PHI in a manner that would violate the HIPAA Rules if done by the County.
- Vendor shall limit its use and disclosure of PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request, consistent with the HIPAA minimum necessary standard.
- Vendor shall not use or disclose PHI for marketing purposes, shall not sell PHI, and shall not use or disclose PHI for underwriting purposes.

11.2 Safeguards

- Vendor shall implement and maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that it creates, receives, maintains, or transmits on behalf of the County, in accordance with the HIPAA Security Rule (45 CFR Part 164, Subpart C).
- Vendor shall conduct and document a risk analysis of its systems that create, receive, maintain, or transmit ePHI, and shall implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
- Vendor shall encrypt all ePHI at rest and in transit using encryption standards consistent with NIST guidelines and the HIPAA Security Rule.
- Vendor shall implement access controls, including unique user identification, emergency access procedures, automatic logoff, and encryption and decryption mechanisms.

11.3 Breach Notification

- Vendor shall report to the County any use or disclosure of PHI not provided for by this Agreement of which Vendor becomes aware, including any Security Incident (as defined in 45 CFR 164.304) or Breach of Unsecured PHI (as defined in 45 CFR 164.402).

- Vendor shall report any Breach of Unsecured PHI to the County without unreasonable delay, and in no event later than twenty-four (24) hours after discovery of the Breach.
- Vendor's notification shall include, to the extent available: the identification of each individual whose PHI has been, or is reasonably believed to have been, affected; a description of what happened; the types of PHI involved; steps Vendor is taking to investigate and mitigate the Breach; and contact information for Vendor's designated representative managing the Breach response.
- Vendor shall cooperate with the County in meeting its notification obligations under the HIPAA Breach Notification Rule (45 CFR Part 164, Subpart D) and shall bear all costs associated with notification, investigation, and remediation to the extent the Breach is attributable to Vendor's acts or omissions.

11.4 Subcontractors

- Vendor shall ensure that any subcontractor that creates, receives, maintains, or transmits PHI on behalf of Vendor for the performance of Services under this Agreement agrees to the same restrictions, conditions, and requirements that apply to Vendor under this Section, by entering into a written agreement that complies with 45 CFR 164.504(e)(1)(ii).
- Vendor shall remain fully responsible for the acts and omissions of its subcontractors with respect to PHI.

11.5 Individual Rights

- Vendor shall make available PHI in a Designated Record Set to the County, or at the County's direction to an individual, within ten (10) business days of request, in order for the County to meet its obligations under 45 CFR 164.524 (access of individuals to PHI).
- Vendor shall make PHI available for amendment and incorporate any amendments to PHI as directed by the County, in order for the County to meet its obligations under 45 CFR 164.526.
- Vendor shall make available the information required to provide an accounting of disclosures in accordance with 45 CFR 164.528.
- Vendor shall document disclosures of PHI and information related to such disclosures as would be required for the County to respond to a request by an individual for an accounting of disclosures.

11.6 County's Obligations

The County shall notify Vendor of any limitations in its Notice of Privacy Practices that may affect Vendor's use or disclosure of PHI. The County shall notify Vendor of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI, to the extent that such changes may affect Vendor's use or disclosure of PHI. The County shall not request that Vendor use or disclose PHI in any manner that would not be permissible under the HIPAA Rules if done by the County.

11.7 Government Access

Vendor shall make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of the U.S. Department of Health and Human Services for purposes of determining the County's and Vendor's compliance with HIPAA.

11.8 Return or Destruction of PHI

Upon termination or expiration of the Agreement, Vendor shall, at the County's election, return or destroy all PHI received from, or created or received on behalf of, the County. If return or destruction is not feasible, Vendor shall extend the protections of this Section to the retained PHI and limit further uses and disclosures to those purposes that make the return or destruction infeasible, for so long as the PHI is retained. This provision shall survive the termination or expiration of the Agreement.

11.9 Term and Termination

The obligations of this Section shall be effective as of the date the Agreement is executed and shall remain in effect for as long as Vendor retains any PHI. The County may terminate the Agreement if the County determines that Vendor has violated a material term of this Section. If cure is not possible, the County shall report the violation to the Secretary of the U.S. Department of Health and Human Services. The respective rights and obligations of Vendor under this Section shall survive the termination or expiration of the Agreement.

Section 12. General Provisions

12.1 Survival

The obligations set forth in this Exhibit, including but not limited to those related to Confidential Information, CJI, PHI, records management, data return and destruction, and indemnification, shall survive the expiration or termination of the Agreement.

12.2 Compliance with Laws

Vendor shall comply with all applicable federal, state, and local laws, regulations, and ordinances, as they may be amended from time to time, including but not limited to the Illinois Local Records Act (50 ILCS 205), the Illinois Freedom of Information Act (5 ILCS 140), the Illinois Personal Information Protection Act (815 ILCS 530), the Americans with Disabilities Act (42 U.S.C. § 12101 et seq.), the Health Insurance Portability and Accountability Act (HIPAA) and associated rules, the FBI CJIS Security Policy, and any rules, regulations, or guidance issued thereunder.

12.3 Subcontractors

Vendor shall ensure that all subcontractors, agents, and third parties performing services or having access to County Data in connection with the Agreement are bound by obligations no less protective than those contained in this Exhibit, including the

requirements of Sections 10 and 11 where applicable. Vendor shall remain fully responsible for the acts and omissions of its subcontractors.

12.4 Right to Audit

The County reserves the right, upon reasonable notice, to audit Vendor's compliance with the requirements of this Exhibit, including inspection of systems, processes, records, and facilities used in the performance of Services. This right extends to audits conducted by the County, the Illinois State Police, the FBI CJIS Division, or the U.S. Department of Health and Human Services, as applicable. Vendor shall cooperate fully with any such audit and shall provide access to relevant personnel, documentation, and systems.

12.5 Interpretation

Any ambiguity in this Exhibit shall be interpreted to permit compliance with the HIPAA Rules, the CJIS Security Policy, the Illinois Local Records Act, and all other applicable legal requirements. In the event of a conflict between the terms of this Exhibit and the terms of the Agreement, the more protective provision with respect to the County's data, records, and legal obligations shall control.

12.6 Amendment

This Exhibit may be amended only by a written instrument signed by authorized representatives of both parties. The parties agree to take such action as is necessary to amend this Exhibit from time to time as required for compliance with HIPAA, the CJIS Security Policy, and any other applicable laws or regulations.