DATA AND SYSTEM SECURITY REQUIREMENTS

ARTICLE 1 – PURPOSE AND SCOPE

A. Data security and privacy for Sensitive Information and Information Resources is extremely important to the Texas Department of Family and Protective Services (DFPS).

B. These Data and System Security Requirements ("Requirements") describes the data security, system security, and privacy obligations of Contractors ("Vendors") and their subcontractors that may connect to DFPS Information Resources and/or gain access to Sensitive Information.

C. Vendors with access to Sensitive Information and/or Information Resources agree to be bound by these Requirements. To the extent applicable, the Vendor also agrees to impose these terms and conditions on any subcontractor(s) retained by the Vendor to provide services under the Contract.

D. These Requirements may be updated from time to time. Vendor is solely responsible for ensuring on-going compliance with all terms contained herein by periodically checking for updates.

ARTICLE 2 – DEFINITIONS

A. Breach

A "Breach" is the actual, or possible exposure of Sensitive Information, regardless of format (electronic, paper, etc.), to an unauthorized person by any means, including the unauthorized action of a person currently authorized to access that Sensitive Information. Examples of a breach include but are not limited to:

1. Losing or misplacing all or part of a case file that contains Sensitive Information;
2. Losing or misplacing an electronic device or record containing Sensitive Information;
3. The acquisition, access, use, or disclosure of Sensitive Information in a manner that compromises the security or privacy of the Sensitive Information; or
4. Any accidental or inadvertent disclosure by a person who is authorized to access DFPS Sensitive Information to another person who is not authorized to access Sensitive Information.
5. Complying with this Contract helps ensure that DFPS meets its statutory responsibility to protect Sensitive Information and Information Resources and report breaches as required by law. Statutory responsibility related to Sensitive Information and Information Resources includes:
    a. Texas Family Code § 261.201
    b. Texas Human Resources Code § 48.101
    c. Texas Administrative Code Title 40 TAC Chapter §§ 700 – 745
        1. Adult Protective Services Case Confidentiality, §§ 705.7101 – 705.7123
        2. Child Care Investigation Case Confidentiality, §§ 745.8481 – 745.8493
        3. Child Protective Services Case Confidentiality, §§ 700.201 – 700.207

B. Sensitive Information

"Sensitive Information" is data that has been designated as private or confidential by law or by DFPS. Sensitive Information includes:

1. "Confidential DFPS Case Records" are Adult Protective Services (APS) case file, a Child Care Investigations (CCI) file, or a Child Protective Services (CPS) case file, Information Management Protecting Adults and Children in Texas (IMPACT) case file, or a Child Protective Investigations (CPI) case file.
2. "Personally identifiable information" (PII) means information that alone or in conjunction with other information identifies an individual, including an individual's:
   - **a.** Name, social security number, date of birth, or government-issued identification number;
   - **b.** Mother's maiden name;
   - **c.** Unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
   - **d.** Unique electronic identification number, address, or routing code; and
   - **e.** Telecommunication access device as defined by Texas Penal Code § 32.51.
3. "Data" includes any information from DFPS such as created or managed business and research data, metadata, and credentials created by or issued on behalf of DFPS. Data also includes:
   - **a.** Protected Health Information (PHI)
   - **b.** Criminal History Record Information (CHRI)
   - **c.** Criminal Justice Information Services (CJIS) Information
   - **d.** Social Security Administration (SSA) Information
   - **e.** Centers for Medicare and Medicaid Services (CMS) Information
   - **f.** Internal Revenue Service (IRS) Federal Tax Information (FTI)

C. Information Resources

"Information Resources" are any devices, networks and related computing infrastructure that DFPS owns, operates, manages, or has obtained for use to conduct DFPS business. DFPS Information Resources include but are not limited to, DFPS-owned or managed storage; processing, communications devices and related infrastructure on which DFPS data is accessed, processed, stored, or communicated, and may include personally owned devices.

ARTICLE 3 – SECURITY PATCHES AND UPDATES

A. The Vendor must apply patches and updates to hardware, applications and/or operating systems used in connection with the services provided to DFPS as follows:

1. The Vendor's internal systems and networks necessary for the Vendor to fulfill its obligations to DFPS must have security patches and functional updates done to its internal systems software and firmware based on the severity established by the Common Vulnerability Scoring System (CVSS).
   - **a.** Low severity vulnerabilities should be patched no more than 90-days of patch/update's commercial release.

b. Medium severity vulnerabilities should be patched no more than 60-days of patch/update's commercial release.

c. High severity vulnerabilities should be patched no more than 30-days of patch/update's commercial release.

d. Critical severity vulnerabilities should be patched as soon as possible and should not exceed more than 30-days of patch/update's commercial release.

2. The Vendor will implement, maintain and use appropriate administrative, technical and physical security measures to protect Sensitive Information. This shall include the use of virus and malware protection software that covers all devices and networks used to perform under this Contract. Vendor shall ensure that this software and virus/malware file definitions are regularly updated per manufacturer's recommendations.

ARTICLE 4 – COMPLIANCE WITH REGULATIONS

A. The Vendor will strive to implement and use industry best practices regarding the collection, access, use, disclosure, safeguarding and destruction of Sensitive Information.

B. The Vendor will have a privacy policy and a prominently-posted privacy statement or notice.

C. The Vendor agrees to comply with all applicable state and federal laws that apply to data and system security as well as privacy including, but not limited to the following:

1. Section 106 of the Child Abuse Prevention and Treatment Act (CAPTA), found at 42 U.S.C. 5106a;

2. Title 1, Texas Administrative Code, Sections 202.1, 202.3 and Subchapter B related to information security standards

3. Texas Human Resources Code, Sections 12.003, 40.005, and Chapter 48;

4. Texas Business and Commerce Code, Subtitle B, related to identity theft;

5. Section 471 of Title IV-E of the Social Security Act, found at 42 U.S.C. 671(a)(8) and related rules found at 45 C.F.R. 1355.30 and 45 C.F.R. 205.50;

6. Texas Family Code, Sections 261.201-.203 related to confidentiality and privileged communication and information about a child fatality;

7. Texas Family Code, Sections 264.408 and 264.511 related to use and ownership of confidential information and records;

8. Family Educational Rights and Privacy Act (FERPA) found at 20 U.S.C. 1232(g) and 34 C.F.R. Part 99;
9. Texas Health and Safety Code, Section 85.115 related to confidentiality of medical information;
10. Title 40, Texas Administrative Code, Subchapter B, related to confidentiality and release of records;
11. Texas Health and Safety Code, Section 81.046 and Chapters 181 related to confidentiality of medical records and 611 related to protection of mental health records;
12. The Federal Information Security Management Act of 2002 (FISMA) found at 44 USC 3541 et seq;
13. Internal Revenue Service Publication 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies and Title 26 USC Internal Revenue Code regarding taxes;
14. National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4 – Recommended Security Controls for Federal Information Systems and Organizations, and Special Publication 800-47 Security Guide for Interconnecting Information Technology Systems; and
15. Federal and State Public Information Acts found at 5 USC 552 and 552a and Texas Government Code Chapter 552.

ARTICLE 5 – UNAUTHORIZED USE, STORAGE OR DISCLOSURE OF INFORMATION

A. The Vendor will not access, use or disclose Sensitive Information other than to carry out the purposes for which DFPS disclosed the Sensitive Information, except as required by applicable law, or as otherwise authorized in writing by DFPS. For the avoidance of doubt, this provision prohibits the Vendor from using, for its own benefit, Sensitive Information or any information that may be derived from it. If required to disclose information by a court of competent jurisdiction or an administrative body, the Vendor will notify DFPS in writing as soon as possible upon receiving notice of such requirement and prior to any such disclosure, unless prohibited by law from doing so.

B. The Vendor transmission, transportation or storage of Sensitive Information (including cloud storage by a third party vendor or subcontractor) outside of the United States, or access of Sensitive Information from outside the United States, is prohibited unless Vendor obtains prior written authorization from DFPS.

C. If Vendor leverages its existing cloud-based services or acquires cloud-based services to perform under this Contract, Vendor must utilize the Federal Risk and Authorization Management Program

(FedRAMP) information security and privacy requirements (including security and privacy controls, and controls selected for continuous monitoring) for cloud services. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

D. Notwithstanding any other requirement contained in this Contract, Vendor acknowledges and agrees that DFPS owns all right, title and interest in any data or Sensitive Information provided to Vendor that is related to any services Vendor may provide under this Contract.

ARTICLE 6 – INFORMATION SECURITY PLAN

A. The Vendor will establish, maintain and comply with an information security plan ("Information Security Plan") which must contain, at a minimum, those elements set forth in this contract. The Vendor Information Security Plan will be designed to:

1. Ensure the security, integrity and confidentiality of Sensitive Information;
2. Protect against any known or anticipated threats or hazards to the security or integrity of such information;
3. Protect against unauthorized access to or use of Sensitive Information including use of an employee security acknowledgment or similar agreement;
4. Reduce risks associated with the Vendor having access to DFPS Information Resources;
5. Provide a plan for disaster recovery and business continuity; and
6. Comply with all applicable legal and regulatory requirements for data protection

B. On at least an annual basis, the Vendor will review its Information Security Plan and update and revise it as needed in order to incorporate new or revisions to controls based on new threats and technology improvements.

C. Upon reasonable notice, Vendor must provide and cause its subcontractors and agents to provide to DFPS or its designee, prompt, reasonable and adequate access to any system security records or documents that are directly pertinent to the performance of the Contract including, but not limited to:

1. Vendor's Information Security Plan, including information security policies and procedures;
2. Vendor logs of system, network or application violation reports;
3. Vendor's employee security acknowledgement agreements; or
4. Lists of Vendor's employees, subcontractors, and agents who have been authorized to have access to Sensitive Information under this Contract.

D. At least annually, the Vendor will perform testing or conduct an audit such as System and Organization Control (SOC) 2 Type II, AICPA SSAE 18 review, or an IT General Controls or Application audit conducted by a certified auditor demonstrating that appropriate network and computing security safeguards and controls are in place and functioning properly. Vendor will provide, and will cause its subcontractors and agents to provide, to DFPS, upon reasonable notice, current, written certification demonstrating that appropriate system, network, and data protection

controls including those controls over data transfers and the handling of PII are in place and functioning properly. Acceptable forms of written certification may include:

1. The American Institute of Certified Public Accountants' Statement on Standards of Attestation Engagements 18 (SSAE 18) or similar subsequent report;
2. General Security Controls Audit performed within one year of DFPS' request;
3. Application Controls Audit performed within one year of DFPS' request; or
4. Vulnerability Assessment such as a network penetration test or other similar assessments.

E. Upon review of any documentation related to system, network or data security, DFPS may require that Vendor make modifications that will ensure better protection of Sensitive Information. However, DFPS review of or failure to review any Vendor documentation will not relieve, waive, or satisfy any of Vendor's obligations under this Contract.

ARTICLE 7 – RETURN OR DESTRUCTION OF SENSITIVE INFORMATION

A. Within 30 days after the termination, cancellation, expiration or other conclusion of this contract or contractual agreement between DFPS and the Vendor, the Vendor will return any and all information supplied by DFPS, unless DFPS requests in writing that such data be destroyed. This provision will apply to all DFPS information (including Sensitive Information) that is in the possession of subcontractors or agents of the Vendor. This provision will also apply to DFPS information stored on routinely backed up media for disaster recovery purposes. Such destruction will be accomplished by "purging" or "physical destruction," in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88. The Vendor will certify in writing to DFPS that such return or destruction has been completed. If the Vendor believes that return or destruction of the information is technically impossible or impractical, the Vendor must provide DFPS with a written statement of the reason that return or destruction by the Vendor is technically impossible. If DFPS determines that return or destruction is technically impossible, the Vendor will continue to protect the information in accordance with the terms of this contract.

B. Data stored on routine back-up media for the purpose of disaster recovery will be subject to destruction in due course of normal Contractor operations. Latent data such as deleted files and other non-logical data types such as memory dumps, swap files, temporary files, printer spool files, and metadata that can customarily only be retrieved by computer forensic experts and are generally considered inaccessible without the use of specialized tools and techniques will not be within the requirement for the return or destruction of data as contemplated by this section. Such archival copies or latent data are subject to the obligations set forth in this Contract for so long as such copies may exist but they shall remain protected as required by this Contract until they no longer exist.

C. Foster Care Litigation. IN ORDER TO COMPLY WITH ONGOING FOSTER CARE LITIGATION INVOLVING DFPS, VENDOR MUST NOT DISPOSE OF OR DESTROY RECORDS PERTAINING TO CHILDREN IN DFPS CONSERVATORSHIP BEFORE

PROVIDING DFPS' CONTRACT MANAGER WRITTEN NOTICE OF ITS INTENT TO DISPOSE OF OR DESTROY RECORDS AND RECEIVING WRITTEN APPROVAL TO DO SO FROM DFPS' CONTRACT MANAGER.

ARTICLE 8 – BREACHES

A. Reporting Breach: The Vendor must notify DFPS' Contract Manager and Office of Information Security (infosec@dfps.state.tx.us) verbally and in writing of any confirmed or suspected breach of its systems that may affect Sensitive Information within one calendar day after discovery of a breach or of receiving notification of a breach. The Vendor report will identify:

1. the nature of the unauthorized access, use or disclosure;
2. the information accessed, used or disclosed;
3. the person(s) who accessed, used, disclosed and/or received information (if known);
4. what the Vendor has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure, and
5. What corrective action the Vendor has taken or will take to prevent future unauthorized access, use or disclosure.

In the event of a confirmed or suspected breach, the Vendor will keep DFPS informed regularly as determined and required by DFPS of the progress of its investigation until the reported breach and all accompanying issues are resolved.

B. Investigation, Response and Mitigation: The Vendor will fully cooperate with DFPS's investigation of any breach experienced by the Vendor. The Vendor's full cooperation will include but not be limited to the Vendor:

1. immediately preserving any potential evidence relating to the breach;
2. promptly (but in no event no later than 48 hours after breach or notification of breach event occurred) designating a contact person to whom DFPS will direct inquiries, and who will communicate the Vendor's responses to DFPS inquiries;
3. as rapidly as circumstances permit, applying appropriate resources to remedy the breach condition, investigate, document, restore DFPS service(s) as directed by DFPS, and undertake appropriate response activities;
4. providing status reports to DFPS on breach response activities, either on a daily basis or a frequency required by DFPS;
5. Coordinating all media, law enforcement, or other breach notifications with DFPS in advance of such notification(s), unless expressly prohibited by law;
6. Ensuring that knowledgeable Vendor staff is available at all times, if needed, to participate in DFPS-initiated meetings and/or conference calls regarding the breach; and
7. DFPS may direct Vendor to provide notification to individuals, regulators, or third-parties including consumer reporting agencies, if applicable, following a breach as required by 15 U.S.C. 7001 et seq. If requested to provide notification, Vendor must comply with all applicable legal and regulatory requirements for breach notification as provided to the

Vendor by DFPS. Vendor will have the burden of demonstrating to DFPS' satisfaction that any required notifications the Vendor is asked to provide was timely made.

8. In the event of a breach involving Sensitive Information, DFPS may, at DFPS' sole discretion and without limitation, do any or all the following:
    a. Require that Vendor obtain cyber security, crime theft and notification expense insurance coverage with policy limits sufficient to cover any liability arising under this Contract, naming the State of Texas through DFPS as an additional named insured and loss payee with primary and non-contributory status;
    b. Require that Vendor indemnify DFPS;
    c. Require that Vendor defend DFPS in any court or administrative proceedings;
    d. Assess liquidated or actual damages, sanctions, or remedies as permitted by the Contract or law.

C. Assistance in Litigation or Administrative Proceedings. The Vendor will make itself and any employees, subcontractors, or agents assisting the Vendor in the performance of its obligations available to DFPS at no cost to DFPS to testify as witnesses, or otherwise, in the event of a breach or other unauthorized disclosure of information caused by the Vendor that results in litigation, governmental investigations, or administrative proceedings against DFPS.

ARTICLE 9 – SYSTEM SECURITY STANDARDS

To the extent that the Vendor electronically stores or transmits Sensitive Information or has access to any DFPS Information Resources, it will include in its written, comprehensive Information Security Plan the establishment and maintenance of a security system covering its computers, including any wireless system that, at a minimum, and to the extent technically feasible, will have the following elements:

A. Secure user authentication protocols including:
1. Control of user IDs and other identifiers;
2. A secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices.

B. Password requirements where passwords must:
1. Contain both upper and lower case characters, such as: a-z, A-Z; (2) have digits and special characters as well as letters, such as: 0-9!@#$ %^&*()_+|~=\`{}[]:";'<>? /;
2. Be at least eight characters long;
3. Not contain consecutive duplicate characters such as: 99 or BB;
4. Not contain consecutive-count numbers or letters such as: 1234 or ABCD;
5. Not be words found in any dictionary, including slang, dialect, jargon, and so on;
6. Not be based on personal information, names of family, and so on;
7. Should be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation; and

8. Should never be the same as your user ID.
9. Control of data security passwords to ensure that such passwords are kept in a location and/or format
10. A requirement that passwords and personal identification numbers (PIN) must not be shared or written down;
11. A requirement that passwords must have an expiration period of at least every 90 days.
12. A requirement that users must change new or temporary passwords when they receive them. The network passwords must be set for one-time use to support this policy.
13. Blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.

C. Secure access control measures that:

1. Restrict access to records and files containing Sensitive Information and systems that may have access to DFPS Information Resources to those who need such information to perform their job duties;
2. Restrict access to active users and active user accounts only;
3. Assign unique identifications plus passwords, which are not vendor/manufacturer supplied default passwords, to each person with computer access;
4. Ensure review of account and account access levels every 12 months, at a minimum;
5. Ensure employee accounts are disabled upon termination; and
6. Ensure all access accounts established for subcontractors, vendors, and/or maintenance accounts are disabled and deleted upon termination or completion of the contract period.
7. Any device that can capture, store, or transmit a still or motion image of any document, person, or environment must have the image-capturing function disabled when the user is operating in any area with access to DFPS information or other restricted DFPS environments. Exemptions to this requirement include dedicated document scanning devices and other equipment designed specifically to capture document images for archival storage.

D. User Controls

1. Users must not purposely engage in activity that may circumvent computer security measures;
2. Users of Information Resources and Sensitive Information must not engage in any act that would violate this Contract;
3. Users must not alter, disable or bypass virus protection software;
4. Automatic updates must be enabled on antivirus protection software.
5. Users are prohibited from installing unauthorized and pirated software on their desktop or laptop computer;
6. Users must be require to either log off or lock access to their workstations before leaving them unattended;
7. All removable media must be scanned for malicious code content before use on any Vendor systems or networks.

E. Encryption

1. Sensitive Information transmitted over external network connections must be encrypted or otherwise similarly protected using HTTPS, FTPS, SFTP or equivalent means;
2. Minimum encryption requirements should be no less than 128 bit key for symmetric encryption and a 1024 (or larger) bit key length for asymmetric encryption;
3. Sensitive Information back-up data must be encrypted;
4. Any type of removable media that contains Sensitive Information must be encrypted and securely stored;
5. All Sensitive Information stored on removable media or portable storage devices must be encrypted using the standards contained in Federal Information Processing Standards (FIPS) Publication 140-2. Removable media or portable storage devices must be scanned for malicious code content before use on any Vendor systems or networks.
6. Emails transmitting any Sensitive Information must be encrypted;
7. Data-at-rest encryption must include the encryption of individual files, portions of the file system (e.g., directories or partitions), or the entire drive (e.g. hard disks or solid-state drives).
8. Stored passwords must be encrypted.

F. Physical Controls:

1. Physical access to all restricted facilities or areas must be documented and managed
2. Physical security systems must comply with applicable regulations such as building codes and fire regulations.
3. Access to information resource facilities must be granted only to authorize personnel whose job responsibilities require access.
4. The process for granting access, by key card or otherwise, to information resource facilities must include the approval of the designated office or staff person responsible for the facility.
5. Access to secured facilities and key cards must not be shared or loaned.
6. Access materials and key cards that are no longer required must be returned r.
7. Users must report lost or stolen access key cards to the building manager immediately upon becoming aware of the loss.
8. Secured facilities that allow visitor access must track that access with a sign in log.
9. Authorized staff must escort visitors to controlled facilities at all times.
10. Facilities must keep access records, entry and exit logs, and visitor logs.
11. Designated staff must deactivate functional capabilities for an access key card upon termination of need.

ARTICLE 10 – INJUNCTIVE RELIEF

Vendor acknowledges and agrees that DFPS may suffer irreparable harm if Vendor or its subcontractors fails to comply with any of the terms of these Requirements or applicable laws. Vendor further agrees that monetary damages may be inadequate to compensate DFPS for Vendor's or its subcontractor's failure to comply with these Requirements. Vendor agrees that DFPS will, in addition to any other remedies available to it at law or in equity, be entitled to seek injunctive relief without

posting a bond and without the necessity of demonstrating actual damages to enforce the terms of these Requirements.