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) describe 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. The Vendor is solely responsible for ensuring ongoing compliance with all terms contained herein by periodically checking for updates.

ARTICLE 2 – DEFINITIONS

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.

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, which includes but is not limited to:

        i. Adult Protective Services Case Confidentiality at §§ 705.7101-7123;

        ii. Child Care Investigation Case Confidentiality at §§ 745.8481-8493; and

        iii. Child Protective Services Case Confidentiality at §§ 700.201-207.

B. Sensitive Information - is data designated as private or confidential by law or 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.

    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. Sensitive Personal Information (SPI)

   c. Criminal History Record Information (CHRI)

   d. Criminal Justice Information Services (CJIS) Information

   e. Social Security Administration (SSA) Information

   f. Centers for Medicare and Medicaid Services (CMS) Information

   g. Internal Revenue Service (IRS) Federal Tax Information (FTI)

C. 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

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:

A. 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).

   1. Low severity vulnerabilities should be patched no more than 90 days after the patch/update's commercial release.

   2. Medium severity vulnerabilities should be patched no more than 60 days after the patch/update's commercial release.

   3. High severity vulnerabilities should be patched no more than 30 days after the patch/update's commercial release.

   4. Critical severity vulnerabilities should be patched as soon as possible and should not exceed more than 14 days of the patch/update's commercial release.

B. The Vendor will implement, maintain, and use appropriate administrative, technical, and physical security measures to protect Sensitive Information. This must include the use of virus and malware protection software that covers all devices and networks used to perform

under this Contract. The Vendor must ensure that this software and virus/malware file definitions are regularly updated per the 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 the 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 5 Recommended Security Controls for Federal Information Systems and Organizations, and Special Publication 800-47 Security Guide for Interconnecting Information Technology Systems.

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. To avoid doubt, this provision prohibits the Vendor from using, for its own benefit, Sensitive Information or any information that may be derived from it.

B. 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 before any such disclosure, unless prohibited by law from doing so.

C. 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 the Vendor obtains prior written authorization from DFPS.

D. In accordance with the Texas Government Code Title 10, Subtitle F, Chapter 2274, Section 2274.0102, it is prohibited for Vendors to enter into any contracts or agreements related to critical infrastructure with certain foreign companies.

1. The Vendor is prohibited from engaging in any contract or subcontract allowing direct or remote access to or control over its critical infrastructure that interfaces with the DFPS information system or any system that stores, processes, or transmits DFPS information. These companies are likely to have direct or remote access to control the infrastructure, potentially threatening national security.

2. The Vendor is prohibited from entering into any agreements, contracts, or purchases of hardware or software from companies that are owned or primarily controlled by citizens from China, Iran, North Korea, Russia, or any other country designated by the Governor under Government Code Section 2274.0103, or if these countries' governments control any companies themselves. This rule applies even if the company or its parent company is publicly traded or listed on a stock exchange.

E. If Vendor leverages its existing cloud-based services or acquires cloud-based services to perform under this Contract, Vendor must use 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 and notify the DFPS Contract Manager of the cloud-based services FedRAMP compliance level.

1. The DFPS Contract Manager must be notified by the Vendor prior to using the cloud-based service.

2. If the Vendor employed cloud-based services prior to their contract with DFPS, the DFPS Contract Manager must be notified of the system's current FedRAMP level.

3. The Vendor must ensure that the cloud-based platform maintains FedRAMP compliance annually and report any major changes to the DFPS Contract Manager.

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

Note: In the 87th Legislative Session, the Texas Legislature passed Senate Bill 475, requiring the Texas Department of Information Resources (DIR) to establish a state risk and authorization management program that provides "a standardized approach for security assessment, authorization, and continuous monitoring of cloud computing services that process the data of a state agency."

To comply, DIR established a framework for collecting information about the cloud service's security posture and assessing responses for compliance with required controls and documentation. Texas Government Code 2054.0593 mandates that state agencies, as defined by Texas Government Code 2054.003(13), must only enter or renew contracts to receive cloud computing services that comply with TX-RAMP requirements beginning January 1, 2022.

For more information, please refer to DIR's Texas Risk and Authorization Management Program (TX-RAMP) website.

F. Notwithstanding any other requirement contained in this Contract, the Vendor acknowledges and agrees that DFPS owns all rights, titles, and interests in any data or Sensitive Information provided to the Vendor that is related to any services the Vendor may provide under this Contract.

ARTICLE 6 – INFORMATION SECURITY POLICY

A. The Vendor will establish, maintain, and comply with an information security policy ("Information Security Policy") 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 the use of an employee security acknowledgment or similar agreement.

4. Reduce risks associated with the Vendor having access to DFPS Information Resources through ongoing risk assessments.

5. Provide a plan for security incidents, disaster recovery, and business continuity.

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 Policy 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, the 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 Policy, including information security policies and procedures.

2. Vendor logs of system, network, or application violation reports.

3. Vendor's employee security acknowledgment 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. Within the first year of the contract and biennial basis thereafter, the Vendor will 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.

The Vendor will conduct a vulnerability assessment, such as a network penetration test, by an external third party on an annual basis to validate that network and computing security controls are in place and functioning properly.

E. The 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 also 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.

Upon review of any documentation related to the system, network, or data security DFPS may require that the 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 the 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 backup 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, THE 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 the DFPS Contract Manager and Office of Information Security 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.

5. What corrective action the Vendor has taken or will take to prevent future unauthorized access, use or disclosure.

The Vendor may report an incident online, by email, or by telephone.

- Online: *Complete the Security Incident Web Based Form*
- Email: infosec@dfps.texas.gov
- DFPS Customer Service Center: 1-877-642-4777

Cybersecurity incident notifications will be treated as confidential under Texas Government Code 552.139, Confidentiality of Government Information Related to Security or Infrastructure Issues for Computers.

B. The Vendor must notify the DFPS Office of Information Security within 24-hours of discovery if the vendor experiences or suspects a breach or loss of PII or a security incident that includes SSA-provided information.

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.

C. 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 a 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, apply appropriate resources to remedy the breach condition, investigate, document, and 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.

7. DFPS may direct the 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, the Vendor must comply with all applicable legal and regulatory requirements for breach notification as provided to the vendor by DFPS. The Vendor will have the burden of demonstrating to DFPS' satisfaction that any required notifications the Vendor is asked to provide were timely made.

   In the event of a breach involving Sensitive Information, DFPS may, at DFPS' sole discretion and without limitation, do any or all of 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 the Vendor indemnify DFPS.

   c. Require that the 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.

D. 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 – MINIMUM SYSTEM SECURITY STANDARDS

If the Vendor electronically stores or transmits Sensitive Information or has access to any DFPS Information Resources, they must have a written and comprehensive Information Security Policy.

This Policy should outline the establishment and maintenance of a security system for their computers. This security system policy should include any wireless system and must have, at a minimum, the following elements:

A. Secure User Authentication Protocols

The Vendor must secure user authentication protocols by implementing cybersecurity best practices. This includes but is not limited to:

1. The Vendor must ensure that their products, services, or information systems are accessed using strong and secure authentication methods. These methods should include phishing-resistant multi-factor authentication (MFA) such as FIDO/WebAuthn Authentication, PKI-based MFA, or Number Matching MFA, biometrics, token devices, or other recognized and secure methods that are resistant to phishing attacks. Email, SMS (or text-based) MFA, or Voice MFA are not approved and should only be used as a last resort while the Vendor moves to a stronger MFA requirement.

2. Protection Against Credential Theft: The Vendor must employ measures to protect user credentials from theft or compromise, including encryption of login credentials during transmission and secure storage.

3. The Vendor must implement continuous monitoring and anomaly detection mechanisms to detect and respond to suspicious or unauthorized authentication activities promptly.

4. Require multi-factor authentication for all remote connections to the Vendor's information systems, like virtual private network (VPN) access and remote access to cloud-based applications.

B. Password Requirements

Ensure that password policies align with the National Institute of Standards and Technology (NIST) Special Publication 800-63B Digital Identity Guidelines authentication and password lifecycle management practices.

1. **Password Length and Complexity**

2. **Passwords used to access the Vendor's information systems must adhere to the following minimum requirements as per NIST guidelines:**

    a. **Minimum Length:** Passwords must be at least eight (8) characters long and allow up to 64 characters for users who use complex passwords or password managers.

    b. **Complexity:** Passwords must include a combination of the following character types:

        i. Uppercase letters (A-Z)

ii. Lowercase letters (a-z)

iii. Numerical digits (0-9)

iv. Special characters (e.g., !, @, #, $, %, etc.)

3. **Prohibited Password Practices**

The following password practices are strictly prohibited:

a. Using common words, phrases, or patterns (e.g., "password," "123456," "qwerty," etc.).

b. Using easily guessable information such as birthdates, anniversaries, names of family members, or publicly available information.

c. Reusing passwords across multiple accounts or systems.

d. Using the same password for an extended period without changing it.

4. **Password Change and Expiry**

To ensure password security, the following practices will be enforced:

a. Implement technology to check passwords against breached password lists and require users to reset compromised passwords.

b. Passwords must be changed every 90 days.

c. Users must be prevented from reusing their last five passwords.

d. Passwords will expire after the specified time limit and require users to create a new password.

e. Block passwords contained in password dictionaries.

f. Disallow consecutive identical characters.

5. **Password Management**

Users are responsible for managing their passwords as follows:

a. Users must not write down or store passwords in an unsecured manner.

b. Passwords must not be shared or disclosed to anyone, including IT staff.

c. Users should immediately report any suspicious activity or suspected compromise of their passwords to the Vendor’s IT support.

C. Multi-Factor Authentication (MFA)

For enhanced security, the Vendor must implement MFA for both local and remote access to all systems, including administrative accounts.

1. **Secure access control procedures:**

    a. Users who require administrative rights to complete their job functions (i.e., IT Staff, software developers, etc.) must maintain a separate administrative account from their mortal (day-to-day) account. The administrative account should be used solely for performing administrative tasks and should not have access to email services.

    b. The administrative account must have a unique password that is distinct from the password of the user's mortal account. The passwords for these accounts must not be identical, and password sharing between accounts is strictly prohibited.

    c. The passwords of the administrative account and the mortal account must be audited regularly. Password auditing must include checks to verify that the passwords for both accounts are not identical. In cases where identical passwords are found, users must be required to reset their administrative account password immediately.

    d. Users with administrative accounts must only use these accounts for performing authorized administrative tasks, such as system configuration, maintenance, and software installations. The administrative account should not be used for day-to-day work, including no email access.

    e. Users with administrative rights must receive role-based training to ensure they understand the importance of this requirement and the security implications of maintaining separate administrative accounts.

    f. 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.

    g. Assign unique identifications plus passwords, which are not vendor or manufacturer-supplied default passwords, to each person with computer access.

    h. Ensure review of account and account access levels every 12 months, at a minimum.

    i. Ensure employee accounts are immediately disabled upon termination.

    j. Ensure all access accounts established for subcontractors, vendors, and/or maintenance accounts are disabled and deleted upon termination or completion of the contract period.

k. The Vendor must make every reasonable effort to prevent users from capturing, transmitting, and storing DFPS data on employee personal devices.

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 required to either log off or lock access to their workstations before leaving them unattended.

7. Employ technical controls to lock unattended devices automatically after 30 minutes of inactivity.

8. 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, SFTP or equivalent means.

2. Minimum encryption requirements should be no less than 128-bit key for symmetric encryption and a 2048 (or larger) bit key length for asymmetric encryption.

3. Backups of Sensitive Information 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 containing Sensitive Information must be encrypted. Consider using data loss prevention tools to automatically encrypt outbound emails based on sensitive information types, such as PII, CJIS, or HIPAA-related data.

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. Business Email Compromise Prevention

The Vendor must implement and maintain the following technologies to help prevent Business Email Compromise (BEC):

1. **Email Authentication and Anti-Phishing Measures**

   Vendors must deploy email authentication protocols such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and/or DMARC (Domain-based Message Authentication, Reporting, and Conformance) to verify the authenticity of email senders and protect against domain spoofing and email impersonation.

2. **Email Filtering and Anti-Spam Solutions**

   The Vendor must utilize email filtering and anti-spam solutions to identify and block malicious or suspicious emails, including phishing attempts, attachments containing malware, and suspicious links.

3. **Advanced Email Threat Protection**

   a. Vendors must implement advanced threat protection mechanisms to analyze email content and attachments for indicators of compromise, malware, and suspicious behavior.

   b. Vendors must implement sandboxing for all content types, including hyperlinks, email attachments, files, and downloads.

   c. The sandboxing technology should provide rapid response mechanisms to quarantine or block malicious content and generate alerts or notifications to appropriate security or IT personnel.

G. 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.

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.

H. Exceptions

If a requirement outlined in Article 9 is not technically feasible, the Vendor must request a technical exception before signing the contract. The request should be submitted to the DFPS Contract Manager, who will work with the DFPS CISO for approval or possible compensating controls. Compensating controls could include providing an alternative means of security. It is important to note that a solution that solves the specific problem will be preferred over a general exemption, as more general exemptions may cause critical data exposures.

ARTICLE 10 – CYBERSECURITY TRAINING

A. The Vendor will comply with Texas Government Code Section 2054.5192, and complete Cybersecurity Training. The Vendor must submit proof of completing and complying with this Article to DFPS as directed.

B. All personnel who access the Vendor's Information Resources must complete cybersecurity awareness training within 30-days of the start date, and thereafter on an annual basis by June 30th of each calendar year. Staff who have direct access to Criminal History Record Information (CHRI) provided by DFPS must also complete FBI CJIS Security Awareness training annually by June 30th of each calendar year, relevant to their level of access. For more information on the appropriate level of training, please reference the FBI CJIS Security Policy, Section 5.2 *Awareness and Training (AT)*, Subsection AT-3, *Role-Based Training*.

C. The Vendor must maintain a list that includes each individual with the date the individual completed the required DIR and/or CJIS cybersecurity training.

D. The Vendor must also maintain a record or other proof of completion of the required Cybersecurity Training in the personnel file of each individual who accesses any of the Vendor's Information Resources.

E. The Vendor must provide role-based cybersecurity training customized to the user's responsibilities and access, in addition to annual training. The primary objective of the role-based training is to equip users with the supplemental knowledge and skills to perform their unique roles securely.

F. Vendors must provide periodic phishing simulations to raise their awareness of email-based threats and to assess their user's ability to recognize and respond to phishing attempts.

G. The Vendor must incorporate lessons learned from internal or external security incidents or breaches into role-based training.

H. The Vendor must periodically broadcast cybersecurity updates, alerts, and best practices to their staff to keep them informed about emerging threats and security measures unique to their organization.

I. Annually during the month of June, the Vendor will certify that all individuals have completed one of the approved cybersecurity training certified by the Texas Department of Information Resources (DIR) at https://dir.texas.gov/sites/default/files/2023-08/FY23-24%20Certified%20Training%20Programs%20V1.pdf, within the past 12 months.

ARTICLE 11 – FBI CJIS SECURITY AND MANAGEMENT CONTROL OUTSOURCING STANDARD

The Contractor must ensure that it or each employee, subcontractor, volunteer, or agent comply with all applicable requirements of the Security and Management Control Outsourcing Standard (Outsourcing Standard) and the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Security Policy if they have access to the following DFPS Systems:

A. Information Management Protecting Adults and Children in Texas (IMPACT).

B. Childcare Licensing Automated Support Services (CLASS).

C. Contractors (and their subcontractors) with direct or indirect access to CJI (e.g., Information Technology support, software, cloud storage, document shredding, document storing, document scanning, media sanitization, etc.).

Additionally, IT staff and IT subcontractors who have a direct responsibility to configure and maintain computer systems and networks for the Contractor that accesses the systems identified above must also comply with all applicable requirements of the Outsourcing Standard and FBI CJIS Security Policy.

The intent of the Outsourcing Standard is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

Please refer to FBI CJIS Policy for more information: https://www.dps.texas.gov/sites/default/files/documents/securityreview/documents/cjissecuritypolicy.pdf

ARTICLE 12 – CJIS MANAGEMENT CONTROL REQUIREMENT

Vendors and Contractors must complete DFPS CJIS Security Checklist with the DFPS Contract Manager to determine whether this Article applies. DFPS will notify any Contractor who must meet and follow the requirements of this Article.

DFPS is authorized by Chapter 411, Subchapter F of the Texas Government Code to receive criminal history record information (CHRI) from the Department of Public Safety (DPS).

The DPS serves as the CJIS Systems Agency for the State of Texas. CJIS Systems Agency (CSA) is a duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the Criminal Justice Information (CJI) from various systems managed by the FBI CJIS.

The primary method of storage of all criminal history record information (CHRI) for DFPS is electronically within the IMPACT application. CJIS information shared through communication mediums must be protected with appropriate security safeguards. The exchange of information may take several forms, including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving, and storing CHRI.

Pursuant to the FBI CJIS Security Policy, Contractor agrees that with respect to the administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the DFPS Network for the interstate exchange of CJIS information, that DFPS will have the authority, via managed control, to set, maintain, and enforce:

A. Priorities.

B. Standards for the selection, supervision, and termination of personnel access CJI/CHRI.

C. Any Policy governing the operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but is not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.

D. Restriction of unauthorized personnel from access or use of equipment accessing the DFPS network.

E. Compliance with all rules and regulations, DFPS policies and CJIS Security Policy in the operation of all information received.

Per Section 5.1.1.4 of the FBI CJIS Security Policy, "…management control of the criminal justice function remains solely with the Criminal Justice Agency."

This Article 11 covers the overall supervision of all DFPS systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any DFPS system to include NCIC Programs that may be subsequently designed and/or implemented within the DFPS.

Article 13 – DATA PROCESSING REQUIREMENTS FOR TECHNOLOGY SYSTEMS

The DFPS maintains a rigorous software approval process to ensure the security, confidentiality, integrity, availability, and compatibility of all software utilized in relation to its operations and data.

All third-party vendors engaged with DFPS are required to adhere to this software approval process prior to the procurement, deployment, integration, or use of any software solutions within the scope of their contractual obligations with DFPS.

A. Notification

Prior to procuring any system or technology solution that will process information provided by DFPS, the Vendor must notify DFPS in writing to their Contract Manager and the DFPS CISO of their intent to do so. The notification should include the following information:

1. A description of the system or technology solution to be procured.

2. The purpose and intended use of the system in relation to DFPS information.

3. The name and contact information of the vendor or supplier from whom the system will be acquired.

4. The expected timeline for acquisition, implementation, and operational use.

This prior notification is necessary for DFPS to ensure compliance with data protection laws and industry regulations, such as TX-RAMP.

Prior to purchasing any system or technology solution designed to process DFPS data, it is mandatory for the vendor to sign and comply with a Memorandum of Understanding (MOU), Data Sharing Agreement (DSA), Data Use Agreement (DUA), and/or Interconnection Security Agreement (ISA). This requirement ensures that the Vendor has a comprehensive understanding of the expectations and requirements pertaining to the protection, transmission, storage, access, and Usage of DFPS data.

B. Approval Process

DFPS will review and assess the proposed procurement's impact on the security, privacy, and compliance of DFPS information. The approval process includes:

1. An evaluation of the security controls and measures that will be implemented to protect DFPS information.

2. An assessment of the system's compatibility with DFPS security policies, standards, and regulatory requirements.

3. A determination of whether the procurement aligns with DFPS's strategic goals and objectives.

4. Consideration of any potential risks associated with the procurement, including data breaches or compliance violations.

C. Written Approval

Upon DFPS's satisfactory review of the proposed system procurement, the Vendor will receive written approval to proceed with the procurement. This written approval must be obtained before any financial commitments are made, contracts are signed, or systems are acquired.

D. Emerging Technology & Approvals

If the vendor plans to utilize any new or emerging technologies, such as Artificial Intelligence (AI), Machine Learning (ML), Application Programming Interfaces (APIs), cloud computing, or any other technology that may process, store, or share DFPS data, it is mandatory first to request written approval from DFPS. The vendor should provide detailed specifications of the proposed technology, its intended use, and any potential associated risks.

ARTICLE 14 – SUPPLY CHAIN & THIRD-PARTY RISK MANAGEMENT

The Vendor must ensure that any third-party contractors or subcontractors they engage in fulfilling their obligations under their agreement with DFPS also comply with the monitoring and compliance standards set forth by the DFPS.

The Vendor's subcontractors must adhere to all relevant laws, regulations, and contractual obligations related to cybersecurity, including but not limited to data protection laws, industry-specific regulations, and contractual agreements with DFPS.

The Vendor will ensure it subcontractors do not enter into any agreements, contracts, or purchases of hardware or software from companies that are headquartered, owned, or primarily controlled by citizens from China, Iran, North Korea, Russia, or any other country designated by the Governor under Government Code Section 2274.0103.

Specifically, the Vendor will ensure its third-party contractors or subcontractors:

A. **Adherence to Cybersecurity Best Practices and Standards**: Ensure that their

subcontractor's practices, processes, and systems are in alignment with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF 2.0).

B. **Annual Review**: The vendor must annually assess and review third-party contractors or subcontractors' compliance with the NIST CSF using the same level of scrutiny as DFPS or higher.

C. **Documentation**: Maintain comprehensive documentation of such reviews and be prepared to present these records to DFPS upon request.

D. **Corrective Actions**: In the event of any non-compliance or deviations from the required frameworks, promptly undertake corrective actions to achieve and maintain compliance.

E. **Notification**: Proactively inform DFPS of any significant changes in their monitoring processes or any findings that may impact the security, integrity, availability, or confidentiality of DFPS data or operations.

F. **Breach and Incident Reporting Requirements**: If any third-party subcontractor working with the Vendor discovers any confirmed unauthorized disclosure, breach, or use of client information, they must immediately report the cybersecurity incident or breach to DFPS. This reporting must occur within 24 hours of confirmation to ensure that DFPS adheres to the breach reporting requirements set forth by the SSA and FBI. The subcontractor must provide all necessary details for investigation and mitigation. The reporting should take no longer than one business day.

Starting September 1, 2023, Texas law mandates businesses and organizations to report any data breach of system security that affects 250 or more Texans as soon as practically possible and no later than 30 days after the discovery of the breach.

DFPS reserves the right to audit, assess, and monitor the cybersecurity practices of third and fourth-party subcontractors to ensure compliance with this policy.

ARTICLE 15 – INJUNCTIVE RELIEF

The Vendor acknowledges and agrees that DFPS may suffer irreparable harm if the Vendor or its subcontractors fails to comply with any of the terms of these Requirements or applicable laws. The Vendor further agrees that monetary damages may be inadequate to compensate DFPS for the Vendor's or its subcontractor's failure to comply with these Requirements. The 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.

Change Log

Revision Date	Revision Version	Revision Notes	Sections Affected
6/15/2019	Ver 1	Document created	
12/10/2019	Ver 1.1	Added cybersecurity training requirement	Article 10
4/1/2021	Ver 2	Major update	• Article 5 • Article 6 • Article 8 • Article 9 • Article 11
8/1/2021	Ver 2.1	Update to cybersecurity training requirement	Article 10
4/3/2022	Ver 2.2	Update to cybersecurity training requirement	Article 10
6/1/2022	Ver 2.3	Update to CJIS requirements	Article 11
5/1/2023	Ver 2.4	Update to cybersecurity training requirement	Article 10
1/15/2024	Ver 3.0	Major Revision to Document	• Article 5 • Article 6 • Article 9 • Article 10 • Article 12 • Article 13
8/20/2024	Ver 3.1	Update to cybersecurity training requirement.	Article 10
10/11/2024	Ver 3.2	Update to FBI CJIS Security Policy link	Article 10.B