southwest key programs

National Headquarters
6002 Jain Lane, Austin, Texas 78721
phone: 512.462.2181 • fax: 512.462.2028 • www.swkey.org

SOUTHWEST KEY GENERAL SYSTEM ACCESS TERMS AND CONDITIONS

1. **Definitions**

   A. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule, published as the Standards for Privacy of Individually Identifiable Health Information in 45 CFR Parts 160 and 164 ("Privacy Rule").

2. **Agreement Precedence**

   A. These Southwest Key General System Access Terms and Conditions (the "Agreement") automatically incorporated into any Statement of Work, Purchase Order, or other agreement for Services between Southwest Key Programs, Inc. ("SWK") and Contractor. Unless agreed to by both parties and explicitly stated to the alternative, in the case of any conflict between this Agreement and any other agreement between SWK and Contractor this Agreement shall control.

3. **Security Risk Management Program –** Contractor agrees to participate in SWK's Contractor Security Risk Management Program including completing SWK's Contractor Security Risk Assessment Questionnaire(s) when requested by SWK. Contractor also agrees to make appropriate resources available for follow-up review(s) of the questionnaire or, if requested by SWK, for an onsite visit.

4. **Protection of SWK Data**

   A. Contractor shall protect against accidental, unauthorized, unauthenticated, or unlawful access, copying, use, processing, disclosure, alteration, transfer, loss or destruction of the SWK Data including, but not limited to, identity theft.

   B. Contractor shall secure and protect SWK Data (or "Data") by using at least the same degree of care as Contractor uses to secure and protect its own Confidential Information but in no event any less than reasonable care consistent with industry best practices for security; provided, however , that with respect to those jurisdictions which do not recognize a reasonable standard of care Contractor shall be obligated to use best efforts.

5. **Risk Assessments**

A. **Risk Assessment** – Contractor shall perform regular, at least annually, comprehensive risk assessments which identify business assets (e.g. facilities, equipment, devices, etc.), the threats against those assets (both internal and external), the likelihood of those threats occurring and the impact upon the organization to determine an appropriate level of information security safeguards.

B. **Risk Mitigation** – Contractor shall manage, control and remediate any threats identified in the Risk Assessment that could result in unauthorized access, copying, use, processing, disclosure, alteration, transfer, loss or destruction of SWK Data so as to achieve the Objectives stated above, commensurate with the sensitivity of the SWK Data, as well as the complexity and scope of the activities of the Contractor pursuant to the Agreement.

C. **Risk Assessment Summary** – Contractor shall provide SWK with a written summary of results of the Risk Assessment upon request. Contractor agrees to remediate any risk findings other than those properly designated as medium or low risk ("high risk findings") from the follow-up assessment that could potentially affect SWK at Contractor expense.

D. **Security Controls Testing** – Contractor shall conduct, at least annually, reviews of security practices against various standards, such as SOC 2 Type II, Payment Card Industry (PCI), as applicable for the hosting service providers and other approved subcontractors involved in delivery of Services. Contractor agrees to remediate any High-Risk Findings resulting from this testing and provide confirmation of remediation to SWK. Upon request, Contractor agrees to make such reports available for review by SWK.

6. **Security Policy**

A. **Security Policy** – Contractor shall have and maintain a comprehensive security policy or policies ("Security Policy") that satisfies the requirements set forth herein. Contractor agrees that it shall not make any change(s) to its Security Policy that effectively reduces or limits the rights or protections offered to SWK under this Agreement.

B. **Production** – Upon request by SWK on an annual basis, Contractor shall provide SWK with a copy of its then current Security Policy. The Security Policy must reflect security measures added as a result of risk assessment findings.

C. **Security Policy Review** – Contractor shall review its Security Policy regularly, at least annually, and particularly following any changes in applicable law, advances in

National Headquarters
6002 Jain Lane, Austin, Texas 78721
phone: 512.462.2181 • fax: 512.462.2028 • www.swkey.org

technology, or changes to Contractor's systems or operations, in order to verify that the Security Policy and controls set out therein remain accurate, comprehensive and up to date.

7. **Organizational Security**

   A. **Responsibility** – Contractor shall assign responsibility for the information security management to appropriate skilled and senior personnel only.

   B. **"Need to Know" Access** – Contractor shall restrict access to information systems used in connection with this Agreement and/ or to SWK Data to only those personnel who are reliable, have sufficient technical expertise for the role assigned and know his or her obligations and the consequences of any security breach.

   C. **Confidentiality** – Contractor Personnel who have access or otherwise been made known of SWK Data, shall maintain the confidentiality of such information for the duration of such individual's employment with Contractor and for a period of three (3) years thereafter. If SWK and Contractor have executed a separate Non-Disclosure Agreement such agreement shall control the duration of confidentiality.

   D. **Required Access** – With respect to any Contractor personnel who no longer require, or is no longer authorized, for whatever reason, access to SWK Data, where access is managed by SWK, Contractor shall notify SWK in writing at least twenty-four (24) hours prior to the date on which such access is no longer required. If such access is removed under exigent circumstances such that twenty-four (24) hours prior notice is not possible, Contractor shall notify SWK immediately upon knowledge that such access is to be removed.

8. **Asset Management**

   A. **Data Security** – Contractor acknowledges that it understands the sensitivity of the SWK Data.

   B. **Data Control** – Unless otherwise agreed to in writing by SWK, Contractor and its personnel shall not copy, download, transmit (to or from), or store SWK Data on any desktop, laptop, server, portable or other device at any location, unless directly related to the delivery of Services.

9. **Security Training**

A. **General** - Contractor shall institute and maintain an appropriate training and education program to ensure that its personnel are appropriately trained regarding the responsibility under the Security Policy and with respect to the confidentiality and nondisclosure duties including, without limitation, any special requirements relating to SWK Data.

B. **Privileged Access Users** - in addition to its training obligations in the agreement generally, Contractor shall make available specific security training to all personnel granted privileged access (e.g. root, DBA, network admin, super user level access, support, etc.) to systems which handle or hold SWK Data and/or are used to provide Services.

C. **Developer** - Contractor also shall make available to development teams associated with development efforts impacting SWK Data and Services specific training focused on well-defined, secure coding standards.

10. **Physical Security**

A. **Securing Physical Facilities** - Contractor shall maintain all systems hosting SWK Data and or providing Services on behalf of SWK in a physically secure environment that restricts access to only authorized individuals and maintains controls to detect any unauthorized access or access attempts. A secure environment includes 24×7 security personnel or equivalent means of monitoring at all relevant locations (including, without limitation, buildings, computer facilities, and records storage facilities).

B. **Physical Security of Media** - Contractor shall prevent the unauthorized viewing, copying, alteration or removal of any media containing SWK Data, wherever located. Removable media on which SWK Data is stored (including removable drives, CDs, DVDs, tape media) must be encrypted using at least 256 bit AES (or equivalent) and may not be used or reused by Contractor to store data of any other customer or to deliver data to any third-party unless prior to such use or reuse, the SWK Data is securely erased.

C. **Media Destruction** - Contractor shall destroy removable media and any mobile device storage (such as USB drives, DVDs, backup tapes, printers, laptops, etc.) containing SWK Data or render SWK Data on such physical media unintelligible and not capable of reconstruction by any technical means prior to any reuse of the media, if requested by SWK or if such media or mobile device is no longer intended for use.

D. **Paper Destruction** - Contractor shall cross shred all paper waste and dispose in a secure and confidential manner to render all paper waste unreadable.

E. **Secure Physical Processing Locations** - Contractor shall keep an up to date record of the location of each data center used in connection with the provision of Services and the owner of such data center and shall provide such record to SWK upon request. Further, Contractor shall promptly notify SWK of any transfer or relocation of material portions of SWK Data.

11. **Communications and Operations Management**

A. **Network Penetration Testing** – Contractor shall, on at least an annual basis, assess current information systems and network having access to, holding, or containing SWK Data. Contractor will provide SWK with a high-level summary of the assessment and confirmation that High-risk Findings have been remediated or a plan (including time frames) is in place to remediate.

B. **Vulnerability Management** – Contractor shall maintain a threat and vulnerability management program including regular vulnerability scanning and remediation of systems, networks, devices, applications, and other assets involved in the storage, transmission, and processing of SWK Data or supporting delivery of Services. Frequency, method, and mechanisms for scanning and resolving, mitigating, and/or patching must be documented.

C. **Data Encryption** – Contractor shall encrypt SWK Data in Contractor's possession or control so that it cannot be read, copied, changed or deleted by unauthorized persons while in storage, including when saved on removable media.

D. **Data Protection During Transmission or Transit** – Contractor shall encrypt and protect SWK Data in Contractor's possession or control so that it cannot be read, copied, changed or deleted by unauthorized persons during transmission or transit inside or outside of Contractor internal network.

E. **Data Loss Prevention** – Contractor shall implement controls and processes to identify and limit inappropriate data loss and exfiltration, and where feasible and appropriate, implement supporting tools and technology for Data Loss Prevention.

F. **Data Destruction** – Contractor shall agree at the request of SWK to (i) promptly return, in the format and on the media reasonably requested by SWK, all or any part of SWK Data; (ii) erase or destroy all or any part of SWK Data in Contractor's possession, in each case to the extent requested by SWK; (iii) provide letter of attestation that data has been successfully erased or destroyed.

G. **Network Security** - Contractor will maintain security of the network and network boundaries, including deployment of relevant technologies (Firewall, IDS/IPS, etc.) to monitor, detect, and prevent compromise of systems, networks, and SWK Data. Firewall configuration and access control lists will be regularly reviewed to limit traffic to essential business operations and those necessary to deliver the Services

H. **Network Ports** – Contractor shall restrict unauthorized network traffic affecting SWK Data.

I. **Malicious Code** – Contractor shall implement a solution to detect and prevent the introduction of malicious code on the information systems handling or holding SWK Data and those involved in delivery of Services, and at no additional charge to SWK, prevent the unauthorized access, disclosure or loss of integrity of any SWK Data and remove and eliminate effects.

12. **Access Controls**

A. **Authorized Access** – Contractor shall maintain the logical separation such that access to all systems hosting SWK Data and/or being used to provide services to SWK will uniquely identify each individual requiring access, grant access only to authorized individuals based on the principle of least privileges, and prevent unauthorized access to SWK Data.

B. **User Access Inventory** – Contractor shall maintain an accurate and up to date list of a personnel who have access to SWK Data and will have a process to promptly disable no more than within twenty-four (24) hours of transfer or termination of access by individual personnel. Personnel must be assigned a unique User ID that is not shared with or used by other personnel.

C. **Password Management** – Contractor communicates new passwords to users in a secure manner with an appropriate proof of identity check of the intended users. Passwords shall not be stored or transmitted in readable form. Password requirements must be complex (composed of letters, numbers, and special characters), no less than 8 characters, changed at a minimum every 90 days, and include account lockout threshold conditions.

D. **Logging & Monitoring** – Contractor shall log and monitor all access to the information system containing SWK Data for additions, alterations, deletions, and copying of SWK Data. The Contractor agrees to maintain full records of system or applicable access attempts, both successful and failed, and upon request will make available to SWK all logs and records. Log event data will be collected, and security alerts generated based

upon active analysis, reporting, and correlation to incident response capabilities. Security administration logs will be retained for a minimum of sixty (60) days and financial/ health care transaction logs will be retained for a minimum of six (6) months (or longer).

E. **Multi-Factor Authentication and Remote Access** - Contractor shall use multi factor authentication for access to Contractor system and when accessing systems containing SWK Data remotely. SMS text messages are not considered an acceptable factor where other means or methods are possible.

F. **Wireless** – Contractor shall ensure the use of Wi-Fi network traffic is encrypted, secured by industry best practices, and regularly monitored.

13. **Use of Laptop and Mobile Devices in Connection with the Agreement**

A. **Secure Environment** – Contractor will maintain SWK Data in secure environment where all secure development, testing, and production databases holding any and all SWK Data shall solely be maintained at all times.

B. **Encryption Requirements** - Contractor shall encrypt the SWK Data on any laptops or mobile devices used by Contractor personnel. Approved and current strong cryptographic control mechanisms must be utilized consistent with industry best practices.

C. **Secure Storage** - Contractor shall require that all laptops and mobile devices be securely stored whenever out of the workforce immediate possession, and in the event of a lost or stolen laptop or other mobile device containing SWK Data, Contractor shall immediately notify SWK.

D. **Network/ Systems Password Storage** - Contractor shall prohibit the use of laptops or other mobile devices to store network or systems passwords that enable access to SWK systems or other systems that handle or hold SWK Data unless such passwords are encrypted and secured.

E. **Remote Wipe/ Inactivity Timeout** – Contractor shall control employee access and implement password controls as well as inactivity timeout of no longer than 30 minutes on all laptops, desktops and mobile devices used by Contractor personnel, and maintain the ability to immediately remotely remove SWK Data from any device lost, stolen, or in possession of a terminated employee.

F. **Laptops/ Mobile Devices** – Contractor shall prohibit access to SWK Data on laptops or mobile devices where above requirements cannot be met.

14. **Information Systems Acquisition Development and Maintenance**

A. **Secure Coding** – Contractor shall disclose what tools are used in the software development environment to encourage secure coding and ensure that all requirements stated, and controls specified within this schedule are incorporated into developed software, applications, and solutions that comprise the Services.

B. **Configuration Management** – Contractor shall use a source code control system that authenticates and logs all changes to the software baseline and all related configuration and build files.

C. **Distribution** – Contractor shall use a build process that reliably builds a complete distribution from source. This process shall include a method for verifying the integrity of the software delivered to SWK.

D. **Disclosure** – Contractor shall maintain an inventory of all third-party software used in developed or provided software and Services, including all libraries, frameworks, components, and other products, whether commercial, free, open-source or closed-source.

E. **Application Penetration Testing** – Contractor shall, on at least an annual basis, assess current information systems applications having access to or holding or containing SWK Data. Contractor will provide SWK with a high-level summary of the assessment and confirmation that high-risk findings have been remediated or a plan including timeframe is in place to remediate.

F. **SWK Data** – SWK Data must be used by Contractor solely for the purposes specified in this agreement. Additionally,

- No production SWK Data shall be used for any purposes other than for delivery of Services (e.g. QA testing, development, user acceptance test areas, training, demonstrations, etc.)

- In instances where production SWK Data is copied to other environments, as authorized by SWK in writing, SWK Data must be copied and transmitted in a secure manner and meet the controls specified with this document. SWK Data must be protected to the same level as applied to the production data or otherwise authorized by SWK and masked or obfuscated data.

- Production environment must be a separate environment from any other non-production environment (e.g. development, UAT, etc.)

G. **Software Patching** – Contractor shell regularly update and patch all computer software and systems that handle or hold SWK Data, with patching for vulnerabilities rated critical or high applied within 30 days of patch availability, unless other controls have been applied that mitigate the vulnerability.

H. **Virus Management** – Contractor shall provide anti-virus and malware software protection to Contractor systems that handle or store SWK Data or support delivery of Services (including laptops and mobile devices), using the most recent distributed version of software including signatures updated at least every twenty-four (24) hours.

15. **Incident Event and Communications Management**

A. **Incident Management/ Notification of Security Incident or Breach** - Contractor shall maintain an approved Incident Response Plan that specifies actions to be taken when the Contractor, one of its subcontractors, or SWK suspects, detects, or has reason to believe that a Security Incident or Breach has occurred or that a party has otherwise gained unauthorized access to SWK Data, systems, or applications containing any SWK Data or supporting delivery of Services. Such Response Plan shall include:

I. **Escalation Procedures** - Escalation procedures must exist to notify senior managers and appropriate reporting to regulatory and law enforcement agencies. Contractor shall immediately report to SWK via telephone or email (and provide a confirmatory notice in writing as soon as practicable but in any event within 24 hours) all incidents that in anyway affect the operation of SWK or the confidentiality, availability or integrity of SWK Data (including backed up data), including but not limited to, any Security Incident, Breach, or successful or attempted unauthorized access to systems or networks which contain or provide access to SWK Data.

II. **Incident Reporting** - Contractor will promptly furnish to SWK full details that the Contractor has or may obtain regarding the general circumstances and extent of such unauthorized access, including without limitation, the categories of personal data, personal health information, and the number and/ or identities of the data subjects affected, as well as any steps taken to secure the SWK Data and preserve information for any necessary investigations.

III. **Investigation & Prevention** - Contractor shall use reasonable efforts to assist SWK in investigating or preventing the reoccurrence of any such access and shall, at its own expense: (i) cooperate with SWK in its efforts to comply with statutory notice or other legal obligations applicable to SWK or its clients arising out of unauthorized access or use and to seek injunctive or other equitable relief; (ii) cooperate with SWK in any litigation and investigation against third parties deemed reasonably necessary by SWK to protect its proprietary rights; and (iii) promptly take all reasonable actions necessary to prevent a reoccurrence of and mitigate against loss from any such authorized access.

IV. **Personnel Training & Confidentiality** - Contractor shall ensure that all personnel fully understand the process and conditions under which they are required to invoke the appropriate incident response. Contractor shall maintain absolute confidentiality regarding actual or suspected authorized possession, use or knowledge of SWK Data or any other failure of Contractor's security measures or non-compliance with its security policies or procedures. Contractor agrees to immediately discontinue use or access to SWK Data, if requested, for any security reasons cited by SWK.

16. **Personal Data Processing** - Contractor shall provide enhanced controls and is responsible for maintaining compliance with all applicable personal data and privacy laws, statutes, regulations, and requirements in so far as the responsibilities for handling and processing included in delivery of Services.

17. **Business Continuity and Disaster Recovery**

A. **Business Continuity and Disaster Recovery Plans** – Contractor shall develop and maintain a business continuity plan and a disaster recovery plan. Contractor must review, update, and test at least annually the business continuity plan and disaster recovery capabilities.

B. **Backups** – Contractor will maintain regularly scheduled backups for all critical information systems and of SWK Data.

C. **Backup Validation** – Contractor will test backup restoration capabilities on a regular basis to ensure SWK Data is available for recovery if needed.

18. **Damages** – Contractor shall indemnify and defend SWK for and against any and all damages (including reasonable attorney's fees) for any claim, allegation, lawsuit, or investigation related in any way to 1) Contractor's breach of this Agreement or 2)

Contractor's negligence, gross negligence, or willful misconduct related to the handling of SWK Data.

19. **Insurance** – Contractor shall maintain Cyber Liability Insurance not less than $2,000,000 per claim for the duration of the Contract and three years following its termination

20. **Subcontracting** – Contractor shall not delegate any Services to be performed under any agreement, purchase order, or statement of work or provide any access to SWK Data or its network to a subcontractor or other third party except to a subcontractor who complies with the security measures at least as stringent as those described in this Agreement and is approved by SWK.

21. **Material Breach** – Any breach of this Agreement by Contractor shall be deemed a material breach under this Agreement and any other agreement which it is incorporated.

22. **Applicable Law** – Contractor shall comply with all applicable laws, rules, regulations, directives and decisions (each, to the extent having the force of law) that are relevant to the handling, processing and use of SWK Data by SWK or Contractor, on SWK's behalf, in accordance with this Agreement