The following are the minimum security requirements for information systems storing, processing, collecting, analyzing, using, evaluating, or transmitting personal identifying information (PII) or sensitive personal information (SPI), as defined in Texas Business and Commerce Code Chapter 521. Respondents must be willing to undergo a risk assessment, including providing a response to a security questionnaire as needed to determine security requirements are met.

1. **Information Security Requirements**:
   - Mobile Security:
     i. Solution must integrate with the Travis County mobile device management solution.
     ii. Vendor must coordinate with Travis County ITS to apply mobile application updates.
     iii. If data falls under CJIS, solution must meet mobile device management requirements in CJIS security policy, version 5-8, section 5.13.2
   - Administrative Access Management:
     i. Solution must employ multi-factor authentication to access administrative side of application.
     ii. Solution must separate administrative functionality from end user functionality.
   - Solution must integrate with Active Directory using SAML 2.0, or comparable
   - Cloud solution infrastructure, if used, must be certified for the type of data that will be hosted (i.e. HIPAA or CJIS)
   - Solution must use trusted TLS certificates.
   - Solution must verify communication between application components, including APIs, are authenticated.
   - Solution must perform input validation to ensure only properly formatted data enters the system.
   - The solution shall generate audit records for defined events that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. Prefer, but do not require, the application to be able to send logs from the application to the Travis County Security Information and Event Management collector.
   - Solution must store user-uploaded files outside of the web root.
   - Solution must provide segregation of components via security control, firewall rules, API gateways, reverse proxies, or cloud-based network security groups.
   - Solution must encrypt data in a manner that is FIPS 140-2 compliant.
   - Emails sent from the system must be able to be encrypted and have the capability to apply an email disclaimer.

- When application is an Infrastructure as a Service (IaaS):
    i. Keep the operating system and application up to date
    ii. Perform backups of the data and supply disaster recovery plan
    iii. Perform security scans of any virtual machines
    iv. Provide tunneling using a virtual private network using IPSec or TLS
    v. Provide a secure terminal if remote access is needed
    vi. Implement defense in depth by providing a firewall and Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)
- When application is a Platform as a Service (PaaS):
    i. Perform vulnerability management on the application using the OWASP Top 10 for the scan policy
    ii. Integrate with Travis County enterprise identity provider using SAML 2.0 and multi-factor authentication
    iii. Encrypt communication for inbound and outbound connections using TLS
    iv. Enable database encryption at rest
    v. Perform database patching when necessary
    vi. Perform vulnerability management on the database
    vii. Perform database hardening before deploying to production
    viii. Perform database access control management according to Travis County policy and standards
    ix. Identify access management roles and responsibilities during the system development life cycle and when in production
- When application is Software as a Service (SaaS):
    i. Perform regular data extractions and backups to a format that is usable without the SaaS provider
    ii. Perform shredding, erasing, and/or crypto shredding for secure destruction of any personal identifying information in production, backups, and archive in accordance with Travis County retention policy
    iii. Data storage and backups within the United States

2. Business Continuity and Disaster Recovery Requirements

- The Vendor, or Supplier's vendors, have and will continue to maintain throughout the Term, detection software, which will send automated alerts to key staff when there is an issue with the IT hardware supporting the provision of Services.
- The Vendor will notify Travis County of any disruption to the Services and will provide regular updates on the workaround being implemented to mitigate disruption and actions underway to resolve the issue, until normal services has been resumed.

- Service level agreements will be included in the contract.
- The Vendor has, and will have in place throughout the Term, a Business Continuity Plan to minimize operational disruption to the provision of service.
- The implementation of the Vendor’s Business Continuity Plan workarounds will be at no additional cost to Travis County.
- The Vendor will have a Disaster Recovery Plan for the application, which includes the procedures needed to recover and restore key parts of the application should they fail.
- The Vendor will perform regular backups and ensure all backups are successfully completed.
- Where a restoration to normal Services requires planned downtime to terminate temporary workarounds implemented to continue services during operational disruption, the Vendor will inform Travis County in advance and agree the date and time of the downtime.
- After disruption to Services, once normal Service has been resumed, the Vendor will promptly complete a root cause analysis report and email it to Travis County- ITS Disaster Recovery. The report will include the cause of disruption, details of how the disruption was resolved and follow-up actions the Supplier will implement to ensure the disruption does not re-occur. The Vendor will also inform Travis County- ITS Disaster Recovery if it is likely the disruption will re-occur.
- The Vendor will test the planned workarounds to services at least once in every twelve months in a controlled environment and will promptly implement lessons learned identified from the test and update the Business Continuity and/or Disaster Recovery Plan accordingly.