Data Security and Risk Management Governance Committee

Article 1. Name, Purpose, Responsibilities

1.1 Data Security and Risk Management Governance Committee

The Data Security and Risk Management Governance Committee. ("Committee") is a standing advisory committee for Williamson County Commissioners Court ("Commissioners Court"), The Committee shall provide County-wide data security strategy recommendations to Commissioners Court for approval. Including but not limited to:

1.1.1 Establish a management framework to initiate and control the implementation and operation of information security within Williamson County's Information Resources

1.1.2 Establish standards regarding the use and safeguarding of Williamson County's Information Resources;

1.1.3 Protect the privacy of individuals by preserving the confidentiality of Personally Identifiable Information entrusted to the Williamson County Systems;

1.1.4 Ensure compliance with applicable Policies and State and Federal laws and regulations, as pertaining to the management of risks and the security of Information Resources;

1.1.5 Appropriately reduce the collection, use, disclosure or retention of sensitive personal information contained in any medium, including paper records;

1.1.6 Ensure accountability;

1.1.7 Educate individuals regarding their responsibilities associated with use and management of Williamson County's Information Resources;

1.1.8 Serve as the foundation for the County's Information Security Program, providing the authority to implement policies, standards and procedures necessary to implement an effective Information Security Program in compliance with this Policy.

1.2 Security Topics

Including but not limited to:

1.2.1 Policy for acceptable use of Information Resources;

1.2.2 Standard Information Security Programs to be adopted County-wide;

1.2.3 Access management and control strategies ;

1.2.4 Administrative/Special access accounts maintenance procedures;

1.2.5 Business Continuity and Disaster Recovery;

1.2.6 Change Management process adoption to ensure secure, reliable and stable operations;

1.2.7 Malware prevention standards to be maintained;

1.2.8 Data Classification Standards to be established to ensure access management and data integrity;

1.2.9 Risk Management Plan to identify accurate inventory and ownership of Information systems and applications;

1.2.10 Safeguarding data confidentiality, encryption/key management using appropriate measures;

1.2.11 Security Incident Management;

1.2.12 Information Services (IS) Security and Privacy rules definition;

1.2.13 Security awareness and privacy training;

1.2.14 System development and deployment standards;

1.2.15 Vendor and Third-Party controls and compliance;

1.2.16 Security control exceptions;

1.2.17 Technology lifecycle (applications and hardware licensing, etc..;

1.2.18 Software lifecycle management updates and patches;

1.2.19 Mobile device management;

1.2.20 Network and wireless architecture;
1.2.21 Configuration Management;
1.2.22 Audit compliance to test/review the program;
1.2.23 Application development (if applicable);

Article 2. Membership

2.1 To be eligible for Committee membership the member must be employed by Williamson County within a department that is exposed to sensitive data, understanding their department's business process around sensitive information.

2.2 The Committee shall be appointed by the Commissioners Court, and may not have at any one time more than one member of the Commissioners Court, if any. The Committee shall be based on the following composition:
Committee Chair;
Williamson County Executive Leadership representing the Commissioners Court;
Williamson County Sheriff's Office;
Williamson County Emergency Medical Services;*
Williamson County Auditor's office *
Williamson County Human Resources *
Williamson County General Counsel
Williamson County Technology Services*
As needed Subject Matter experts (non-voting)
*Court approved in 2003, Williamson County is HIPAA Hybrid Covered Entity

2.3 In the case of a vacancy, the Commissioners Court shall appoint a replacement to serve for the remainder of the unexpired term;

2.4 HIPAA designated department must have a Committee representative;

2.5 Technical solutions required for compliancy are the sole discretion of the Technology subject matter expert;

2.6 The Secretary shall maintain attendance records documenting Committee member absences. If a member is unable to attend a scheduled meeting, they must notify the Secretary prior to the meeting to receive an excused absence; and the notification submitted in enough time to ensure there will be a quorum. Non-attendance at a Committee meeting without notification to the Secretary is an unexcused absence. If a member is unable to attend a meeting, the Committee member may send a representative in their place. This representative may participate but does not have voting rights.

2.7 Within one calendar year, a member who misses the greater than 50% of the meetings scheduled or two consecutive meetings with at least one unexcused absence is subject to removal from the Committee. The Secretary will notify the member of the removal.

Article 3. Chairperson Responsibilities and Delegation of Authority

3.1 The Chair shall preside at all meetings of the Committee. The Chair shall represent the Committee in presentations to the Commissioners Court, unless the Chair delegates this duty to another member.

3.2 In the case of a tie during a vote at which a quorum is present, the Chair has the authority to break the tie.

3.3 The Executive Leadership Representative shall perform all the duties of the Chair in the case of absence or disability and such other duties as may arise, from time to time, when requested by the Committee.

3.4 The Committee Chair will present policies to Commissioners Court for approval.

3.5 In the case where the security risks are too high to wait on the Committee review, the Sr. Director of Technology Services or Commissioners Court Executive may make policy immediate.

Article 4. Meeting

4.1 The Committee regular business meeting schedule shall be determined by the Committee with meetings to be held a minimum of once every three months. The schedule shall be determined and distributed, to include location, date, and time, by the Committee Chair.

4.2 Meeting agendas are the responsibility of the Committee Chair.

4.3 The Secretary will prepare the written notice, including an agenda, for each regular meeting and electronically transmit notice and agenda to each Committee member at least five business days before the meeting date.

4.4 Any Committee member may call a special meeting of the Committee.

4.5 The only business considered at a special meeting shall reasonably relate to the purpose or purposes described in the request for the special meeting.

4.6 Special meetings require at least 72 hours prior notice to the Committee members.

4.7 A majority of the total voting membership, excluding vacancies, constitutes a quorum for conducting Committee business.

4.8 A majority vote of the members present at a meeting at which a quorum of voting members is present is necessary for action by the Committee. During a meeting at which a quorum has been established, and then subsequently lost due to members leaving, results in postponement of all remaining business items requiring a Committee vote or action until the quorum is reestablished or the next scheduled meeting at which a quorum is established.

4.9 A Committee member may not transfer voting rights by proxy.

4.10 Minutes of the Committee meetings, documents distributed and other records will be available to the committee members through the Committee's SharePoint site.

4.11 Committee members should maintain objectivity and professionalism when carrying out business of the Committee.

Article 5. Amendments

5.1 Changes to these bylaws should be given to all stakeholders in a timely manner prior to the changes being voted on.

5.2 The Committee may recommend amendments to these bylaws at a regular or special meeting. The notice of the meeting must include the written text of any proposed amendment(s). The minutes of the meeting must include the final written text of a proposed amendment as recommended for adoption. An amendment recommended by the Committee is not effective unless approved by the Commissioners Court.

5.3 An amendment to the bylaws takes effect when approved by the Commissioners Court unless the amendment specifies a later effective date.

5.4 The Secretary will distribute amended copies of the bylaws to Committee members.

Article 6. Applicability

6.1 All organizational units within Williamson County

6.2 All Information Resources owned, leased, operated , under the custodial care of , or connected to any Williamson County organization, resource or facility;

6.3 All Information Resources owned, leased, operated, or under the custodial care of third-parties operated on behalf of a Williamson County, organization, or facility; and

6.4 All individuals accessing, using, holding, or managing Information Resources on behalf of Williamson County.

6.5 All devices using the County's Infrastructure.

Data Security and Risk Management Governance Committee

Article 7. Applicable Policies and State and Federal Laws

including but not limited to:

7.1 Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, and all regulations adopted to implement FERPA.

7.2 Health Insurance Portability and Accountability Act of 1996 (HIPAA)

7.3 Health Information Technology for Economic and Clinical Health Act, (HITECH) Act of 2009

7.4 Federal Privacy Act of 1974 and amended by CMPPA of 1988

7.5 Social Security Act, 42

7.6 Gramm-Leach-Bliley Act (GLBA Gramm-Leach-Bliley Act (GLBA)

7.7 Texas Government Code

7.8 Texas Business and Commerce Code

7.9 Texas Government Code Section

7.10 Texas Administrative Code

7.11 Criminal Justice Information System (CJIS)