Chapter 136. Acceptable Use of Information Technology[1]

Contents:

Subchapter A. General Provision of Chapter 2

136.001 Authority 2
136.002 Purpose of Chapter 2
132.003 Application of Chapter 2
136.004 Effective Date 2
136.005 Definitions 2
[136.006-136.013 Reserved] 3

Subchapter B. General Application of Acceptable Use Policy 3

132.014 Policy Violations 3
136.015 Technology and Operations Responsibilities 3
136.016 Department Responsibilities 3
136.017 Responsible Use of IT Resources by Users 4
136.018 No Expectation of Privacy 5
136.019 Periodic Monitoring 5
136.020 Data Ownership 5
136.021 Records Retention 5
136.022 User IDs and Passwords 5
136.023 Occasional and Incidental Personal Use 6
[136.024-136.034 Reserved] 6

Subchapter C. Use of Email, Data, Applications, & Equipment 6

136.035 Email Use 6
136.036 Applications and Data 7
136.037 Laptops, Tablets, or Portable Storage 8
136.038 Remote Access 8
[136.039-136.049 Reserved] 9

Subchapter D. Artificial Intelligence (AI) 9

136.050 Approved AI Tools 9
136.051 Use Cases 9
136.052 Protection of County Information 9
136.053 Human Judgment and Oversite 9
136.054 Disclosure of AI Use 10
136.055 AI-Generated Content and Public Information 10
136.056 AI Awareness Training 10
136.057 Department Responsibilities for AI Use 10
136.058 Additional Information 10
[136.059-136.069 Reserved] 10

Subchapter E. Web Content, Social Media 10

136.070 Internet and Networks 10
136.071 Inappropriate Content 11
136.072 Web Content Accessibility 11
136.073 Social Media Use 11

[1] Chapter 136 was adopted by Travis County Commissioners Court on October 27, 2026, item 52, with an effective date of October 27, 2026. The Acceptable Use of Information Technology Policy was adopted as part of Chapter 110 on October 31, 2017, Item 16 Revised, then amended and incorporated into Chapter 136 on 10/27/2026, item 52.

Subchapter A. General Provision of Chapter

136.001 Authority

The Commissioners Court acting in its capacity as the governing body of Travis County adopts this chapter under the authority of the laws of Texas.

136.002 Purpose of Chapter

The purpose of this chapter is to outline acceptable use of Travis County's information technology (IT) resources. These rules are in place to protect employees, constituents, and Travis County. By establishing and maintaining compliance with this policy, risks and costs to the County are minimized.

132.003 Application of Chapter

All County users granted access to County IT resources must read and understand this subchapter and conduct their activities in accordance with its terms. This policy also applies to virtual/remote users.

136.004 Effective Date

This chapter is effective upon adoption by the Commissioners Court.

136.005 Definitions

In this Chapter:

(1) "Artificial intelligence (AI)" means a computer system that gathers and analyzes information to identify patterns, learn, and make predictions, recommendations, or decisions. AI-generated information or recommendations may be inaccurate or incomplete, so human judgment and oversight are necessary when using AI to make decisions or take actions that affect real-world situations or digital environments.

(2) "Criminal History Record Information (CHRI)" means data collected about an individual's arrests, charges, and convictions.

(3) "Criminal Justice Information (CJI)" means data collected by FBI, CJIS and other law enforcement agencies necessary for law enforcement and civil agencies to perform their duties.

(4) "Health Insurance Portability and Accountability Act (HIPAA)" means a U.S. law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers.

(5) "IT Resources" means any County-owned computer device, data, application, and the supporting networking infrastructure.

(6) "Payment Card Industry Data Security Standard (PCI DSS)" means a set of standards developed to encourage and enhance payment card account data security and facilitate the adoption of consistent data security measures globally.

(7) "Personal Identifiable Information (PII)" means any data that could potentially identify a specific individual.

(8) "Protected Health Information (PHI)" means individually identifiable health information.

(9) "User" means any regular or temporary employee, contractor, consultant, vendor, volunteer, student intern, or other person granted access to IT resources.

[136.006-136.013 Reserved]

Subchapter B. General Application of Acceptable Use Policy

132.014 Policy Violations

(a) Violators of this policy may be subject to disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil. See chapters 109, 110, and 120 of the Travis County Code.

(b) The appropriate HR Liaison for the department or office will investigate reports or complaints of possible violation of this policy. This would be in collaboration with the department having ownership of the IT resources used and consultation from Enterprise Risk Management and/or other departments as appropriate.

136.015 Technology and Operations Responsibilities

Technology and Operations will secure, routinely monitor, and log applications and IT resources.

136.016 Department Responsibilities

(a) Management shall ensure that all users are aware of and comply with this policy. It is management's responsibility to notify their HR Liaison for users possibly engaging in inappropriate or unauthorized use of IT resources.

(b) Supervisors shall ensure users are appropriately trained and educated on acceptable use policy. They should monitor user's activities to ensure compliance.

136.017 Responsible Use of IT Resources by Users

(a) Users must understand this policy, including acceptable and inappropriate uses in general. All users must comply with federal, state, and local law and all Travis County policies.

(b) Users must practice safe computing. Those accessing department information systems must use caution and exercise good security practices to ensure the protection of department information systems and data.

(1) Do not put confidential or controlled data into any Artificial Intelligence (AI) system. This includes typing, uploading, copying, or pasting it. If unsure whether the information falls under either category or whether an action will be sent to an AI system, ask the Enterprise Risk Management team.

(2) Users who handle sensitive data must position their monitor(s) so that others cannot readily view the information or other reasonable measures to ensure privacy protections as necessary. Examples of sensitive data include Personally Identifiable Information (PII), Protected Health Information (PHI), Payment Card Industry Data Security Standard (PCI DSS) data, Criminal History Record Information (CHRI), and Criminal Justice Information (CJI), or any information not already public.

(3) Users must lock or log off their workstations when walking away.

(4) Users who suspect their device is infected with a virus or malicious software must notify ITS Helpdesk for assistance.

(5) Users must report any weakness in computer security or data privacy, suspicious behavior of others, and any incidents of possible misuse or violation to the ITS Helpdesk.

(6) Users must not tamper, disengage, or otherwise circumvent any County or third-party security controls.

(7) Unauthorized access, interception, modification or destruction of any computer, computer system, department information system, computer programs or data is strictly prohibited.

(8) Users must not use peer-to-peer file sharing technology for unauthorized distribution, display, performance, or reproduction of copyrighted work.

(9) Users must not cause disruption of computers, computer systems or department information systems.

(10) Users must not view, store, or transmit any pornography or other offensive, intimidating, hostile or otherwise illegal material.

(11) Users must not use or distribute unlicensed software, copyrighted materials, or communications of proprietary information.

(12) Users must not access or release any confidential data they do not have authorization to retrieve.

(13) Users must not use County IT resources for commercial financial gain or to conduct and support personal business ventures.

136.018 No Expectation of Privacy

Except for any privilege or confidentiality recognized by law, individuals have no legitimate expectation of privacy during any use of Travis County's IT resources or in any data on those resources. Any use may be monitored, intercepted, recorded, read, copied, accessed, printed, or captured in any manner including in real time, and used or disclosed in any manner, by authorized personnel without additional prior notice to individuals.

136.019 Periodic Monitoring

Periodic monitoring will be conducted of systems used, including but not limited to all computer files, and all forms of electronic communication (including email, text messaging, instant messaging, telephones, computer systems and other electronic records). In addition to the notice provided here, users are notified with a warning banner text at system entry points where users initially sign on about being monitored and are reminded that unauthorized use of IT resources is not permissible.

136.020 Data Ownership

All information created, transmitted, acquired, downloaded, or uploaded via the County's network, internet or intranet is the property of Travis County.

136.021 Records Retention

Files, emails, attachments, and other records are retained, preserved, and/or disposed of in accordance with the County Records Retention Schedule.

136.022 User IDs and Passwords

(a) Individual accountability is required when accessing all IT resources and County information. Everyone is responsible for protecting against unauthorized activities performed under their user ID.

(b) Individual user IDs, passwords, voicemail PINS or any other access codes must be confidential and must not be shared or revealed to anyone except the authorized user. Users must not write down their passwords.

(c) Users must not save, store, or autofill County passwords or other authentication credentials using a web browser's built-in password manager. County passwords and credentials must be stored and managed only through the County-approved password managers as listed in the Technology Standards. Users are responsible for following all County

requirements for protecting passwords and authentication credentials as stated in the Password Standard. These standards are found on TravisCentral.

(d) Users must never disclose their User ID or passwords.

136.023 Occasional and Incidental Personal Use

Occasional, incidental, and necessary personal use of IT resources is permitted, provided such use is otherwise consistent with this policy, is limited in amount and duration, and does not impede the ability of the individual or other users to fulfill Travis County's responsibilities and duties, including but not limited to, extensive bandwidth, resource, or storage utilization. Exercising good judgment regarding occasional and incidental personal use is important.

[136.024-136.034 Reserved]

Subchapter C. Use of Email, Data, Applications, & Equipment

136.035 Email Use

(a) Confidential Data

(1) Users must only send confidential data by electronic communications if they have a business need. Additionally, if users have a business need that requires sending confidential data to an external source via electronic communications, they must use an encryption method.

(2) Users must not transmit restricted confidential information to or from personal email accounts or use a personal email account to conduct business unless explicitly authorized. Users must also not use anonymous email addresses for sending or receiving email or messages.

(b) Users must use caution when opening email attachments or following hypertext links received from unknown senders.

(c) Users must not send unsolicited commercial emails or messages in bulk, also known as spam. They must also not create or forward chain letters of pyramid schemes.

(d) Users must not modify or delete email or messages originating from another person or computer with the intention of deceiving.

(e) Users must not use County IT resources to falsify email or message headers or routing information to hide the original sender.

136.036 Applications and Data

(a) Users will only access County data provided to them as needed to perform their jobs.

(b) Users must not store restricted Travis County controlled, confidential or sensitive information on a non-County issued device, or with a third-party file storage service that has not been approved for such storage by Travis County.

(c) Users can store Travis County data in Microsoft's OneDrive cloud storage since this is an approved solution. However, users must not store confidential Travis County data, such as Personally Identifiable Information (PII), Protected Health Information (PHI), Payment Card Industry Data Security Standard (PCI DSS) data, Criminal History Record Information (CHRI), and Criminal Justice Information (CJI), or any information not already public in unapproved cloud storage services, such as Google Drive.

(d) The use of all local file storage services must comply with all laws and regulations governing the handling of data that includes Personally Identifiable Information (PII), Protected Health Information (PHI), Payment Card Industry Data Security Standard (PCI DSS) data, Criminal History Record Information (CHRI), and Criminal Justice Information (CJI), or any information not already public that is owned or collected by Travis County.

(e) Users must not install software programs that are not authorized, modify existing software, or knowingly violate any licensing agreement.

(f) Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any Travis County computer or network.

(g) Users must use SFTP (secure file transfer protocol) to upload or download files that includes Personally Identifiable Information (PII), Protected Health Information (PHI), Payment Card Industry Data Security Standard (PCI DSS) data, Criminal History Record Information (CHRI), and Criminal Justice Information (CJI), or any information not already public.

(h) Users must not upload Travis County data onto public sites that allow anyone to download files.

(i) Users must not share credit card data using unencrypted methods (unsecure web (http), instant messaging (IM), faxing to public offices/facilities, etc.).

136.037 Laptops, Tablets, or Portable Storage

(a) Users are routinely assigned or given access to IT equipment in connection with their official duties. This equipment belongs to Travis County and must be immediately returned upon request or at the time a user is separated from the County.

(b) Any County-owned laptop, tablet, phone, or two-factor authorization security key (i.e. YubiKey) that is lost or stolen must be reported to the ITS Helpdesk as soon as possible.

(c) Only removable storage devices (i.e., USBs, SD cards, external hard drives) that have been purchased by Travis County may be connected to Travis County devices. If unsure, please contact ITS or department IT Staff. ITS may contact users directly to confirm the removable storage device belongs to Travis County.

(d) Any removable storage devices that contain regulated data, including Personally Identifiable Information (PII), Protected Health Information (PHI), Payment Card Industry Data Security Standard (PCI DSS) data, Criminal History Record Information (CHRI), and Criminal Justice Information (CJI), or any information not already public, must be encrypted, tracked, physically labeled, and purchased by Travis County.

136.038 Remote Access

(a) Users must provide a secure space at their remote work location where household members or others cannot see or overhear conversations or interactions. Use headset/earbuds whenever possible.

(b) Users must provide a secure and appropriate level of internet connectivity at their remote work location.

(c) Users must use only approved software when connecting to Travis County network. If they are using their own computer, they must be running current virus protection software.

(d) Users are responsible for ensuring the confidentiality, safety, and integrity of data, documents, and software used at the remote work location.

(1) Do not put any confidential documents in personal or public trash. Bring documents to the office and place them in the approved bins for shredding.

(2) If printing confidential documents from a home printer:

(A) Pick up all printed items promptly and store them securely.

(B) Do not leave them on the printer for others to find and see the content.

(C) If possible, locate the printer near for close monitoring.

(e) Users must not copy, move, or store confidential data onto local hard drives or removeable electronic media, unless explicitly authorized for a defined business need.

[136.039-136.049 Reserved]

Subchapter D. Artificial Intelligence (AI)

136.050 Approved AI Tools

(a) All new AI technology must be submitted for review through the Technology Assessment Program before consideration of implementation. The use of unapproved AI tools is prohibited.

(b) All AI tools must be accessed exclusively through County technology platforms, systems, and applications that are listed in the Technology Standards.

136.051 Use Cases

Users may use AI for research, drafting, translation, summarization, analysis, and productivity assistance when doing so complies with this policy and no prohibited data is shared.

136.052 Protection of County Information

(a) Do not enter controlled or confidential information into any AI system this includes Personally Identifiable Information (PII), Protected Health Information (PHI), Payment Card Industry Data Security Standard (PCI DSS) data, Criminal History Record Information (CHRI), and Criminal Justice Information (CJI), or any information not already public.

(b) If unsure whether information is controlled or confidential, see the Data Classification and Protection Policy found on TravisCentral.

136.053 Human Judgment and Oversite

(a) All AI outputs must be reviewed for bias or harmful content before use.

(b) The County complies with the DIR AI System Code of Ethics (fairness, accountability, transparency, explainability, human oversight) for all procured, developed, deployed, or used AI systems.

(c) AI may inform decisions, but for consequential matters the County must ensure meaningful human review and the opportunity for residents to seek human reconsideration.

136.054 Disclosure of AI Use

(a) Clearly label AI-assisted or AI-generated content used in external communications.

(b) Any public-facing AI system (for example, a website chatbot, reports, recommendations, or decisions) must provide clear, conspicuous disclosure that the resident is interacting with AI.

(c) Users must not present AI-generated work as their original work.

136.055 AI-Generated Content and Public Information

AI prompts, outputs, and final work products created and used for County business are public records subject to the Texas Public Information Act (PIA).

136.056 AI Awareness Training

(a) All personnel must complete the required annual AI Awareness Training.

(b) Any AI-related incident, policy violation, misuse, malfunction, data exposure, security concern, integrity issue, or evidence of biased or discriminatory outputs must be reported immediately to Enterprise Risk Management.

136.057 Department Responsibilities for AI Use

(a) Departments remain responsible for decisions informed by AI, and personnel maintain full authority to review, validate, and override AI-generated outputs.

(b) Departments must ensure AI use does not impede compliance with public information, records retention, or legal hold requirements.

136.058 Additional Information

Refer to the Travis County AI Guidelines found on TravisCentral.

[136.059-136.069 Reserved]

Subchapter E. Web Content, Social Media

136.070 Internet and Networks

(a) Users who access the internet with Travis County IT Resources do so at their own risk. Travis County is not responsible for material viewed, downloaded, or received by users through the internet.

(b) The ability to connect with a specific website does not imply that users of Travis County systems are permitted to visit or download files from that site.

(c) All users accessing the internet with County IT resources should demonstrate professionalism, respect and good judgment, observing County policies against harassment, discrimination and inappropriate conduct.

136.071 Inappropriate Content

(a) The County may block access to web content it deems as inappropriate, or filter emails destined for County mailboxes.

(b) The County shall not be responsible for material viewed or downloaded by users from the Internet or messages delivered to a user's mailbox.

(c) Users are cautioned that many Internet pages and emails include offensive, sexually explicit, and inappropriate material. It is not possible to always avoid contact with offensive content on the Internet or in County email. If such an action occurs users are expected to delete the offensive material, leave the offensive site, and contact the ITS Helpdesk.

136.072 Web Content Accessibility

(a) All digital content made available to the public such as websites, mobile applications, documents, forms, social media posts and other communications must conform to Web Content Accessibility Guidelines (WCAG) 2.1 or higher, Level A and AA, consistent with the Americans with Disabilities Act Title II (28 CFR §§ 35.200-35.201).

(b) Users who create, publish, or distribute such content on behalf of the County are responsible for ensuring it meets this standard.

136.073 Social Media Use

(a) Any creation of new social media accounts used to represent Travis County must be coordinated through Travis County's Public Information Office (PIO). This applies only to County departments that report directly to Commissioners Court. This does not apply to Elected/Appointed Officials.

(b) Social Media used to represent Travis County belongs to Travis County. Posts that contain confidential information, such as Personally Identifiable Information (PII), Protected Health Information (PHI), Payment Card Industry Data Security Standard (PCI DSS) data, Criminal History Record Information (CHRI), and Criminal Justice Information (CJI), or any information not already public are prohibited.