809 Information Technology And Services Usage Policy (Revised) 20250219

I. Overview and Scope

This policy outlines acceptable use of technology resources at the Baptist General Convention of Texas (Texas Baptists), and aligns with the organization's established culture of ethical and lawful behavior, openness, trust, and integrity.

To support its ministries, Texas Baptists provides various technology tools and systems, with a focus on balancing security and usability.

All users, including employees, contractors, consultants, volunteers, occasional workers, and other individuals working at Texas Baptists, as well as personnel affiliated with third parties, must comply with this policy. The policy applies to all information assets and technology tools owned or leased by Texas Baptists, cloud-based systems, and devices that connect to a Texas Baptists network or reside at a Texas Baptists site.

II. Texas Baptists IT Policy

A. Security

As a Texas Baptists technology resource user, you are responsible for exercising good judgment and complying with all Texas Baptists policies and guidelines. Any suspected security issues, including malware, must be reported immediately to the IT Helpdesk.

Your password is confidential and should only be shared with Texas Baptists IT User Support staff for support purposes. To maintain security, you should never write down or store your password where others can find it, and you can't share it with other users unless directed by IT. Texas Baptists IT may also require you to change your passwords periodically.

Through legal or technical means, you must ensure that proprietary information stays within the control of Texas Baptists at all times. Conducting Texas Baptists business that results in the storage of proprietary information on personal or non-Texas Baptists controlled environments, including third-party devices without a contractual agreement with Texas Baptists, is prohibited.

Texas Baptists systems are strictly prohibited from storing sensitive information without explicit approval. This includes, but is not limited to: Private Health Information (PHI), Financial Information such as credit cards, and Personally Identifiable Information (PII) such as Social Security Numbers (SSNs) and driver’s license numbers.

Any exceptions to this policy must be in full compliance with all applicable laws and regulations, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry (PCI). Unauthorized storage of sensitive information can result in significant legal and financial consequences for both the individual and Texas Baptists. Following this policy is crucial to protect both the organization and the individuals it serves.

B. Cloud, SaaS, and Software

Texas Baptists collaborates with and depends on partners who provide IT resources, applications, storage, etc. All cloud, SaaS, and third-party providers and tools must be reviewed, approved, and tracked by Texas Baptists IT.

To ensure the financial integrity and security of Texas Baptists, any cloud-based or software applications utilized by this organization that are involved in the processing of financial transactions, including but not limited to the acceptance of payments, donations, outgoing payments,or any other form of monetary exchange, must be processed through existing systems in place, which are under the oversight of the Controller.

Texas Baptists aims to maintain the highest standards of financial accountability and transparency while safeguarding the assets entrusted to the organization by its supporters and stakeholders.

Nonstandard software necessitates special handling, installation, and potential compatibility and security testing with existing systems, which may incur additional costs for the department. These costs may include but are not limited to:

- Procurement of software licenses
- Configuration and Installation
- Integration with existing systems
- Compatibility and security testing
- Additional hardware requirements
- Specialized training for staff
- Ongoing maintenance and support

Therefore, to ensure responsible and efficient resource allocation, departments will be charged back for any expenses directly associated with the acquisition and implementation of nonstandard software.

All software installed on Texas Baptists devices must be used in compliance with all applicable licenses, notices, contracts, and agreements.

Texas Baptists IT must approve all SaaS (Software as a Service) applications, including web-based software and software that exclusively uses the internet, before use. To obtain approval for ministry required SaaS, contact Texas Baptists IT. The nonstandard software approval process will be used for SaaS approval. Any associated purchase or subscription costs for approved SaaS must be paid by your ministry using approved payment methods.

Texas Baptists approved SaaS is restricted to ministry use only. You must not use your Texas Baptists email address for personal SaaS activities, including Banking, Shopping, Insurance, Healthcare, Newsletters, and more.

This Texas Baptists policy expressly forbids installation of the following:

- Privately owned software
- Software not approved by Texas Baptist IT
- Pirated copies of any software titles
- Any software that is not licensed to Texas Baptists
- Any software not installed according to the procedures set out in this policy.

Your business documents and data belonging to Texas Baptists must be stored in approved cloud storage and network storage environments. Any data stored on personal computers will not be backed up.

You must not store personal photos, videos, music, or other personal data on Texas Baptists cloud or network locations. Your personal files stored on devices such as laptops, tablets, or phones will not be transferred by Texas Baptists IT when moving you to a new device.

C. Email

As a Texas Baptists user, you are expected to check your Texas Baptists administered email account and read Announcements daily when working. This ensures that all users are up-to-date on important organizational information and can respond to communications in a timely manner.

All Texas Baptists ministries must use email accounts administered by Texas Baptists IT for organizational business. This policy is in place to maintain security and control over sensitive information. The use of personal or external email accounts for organizational business is strictly prohibited, unless explicitly approved by Executive Leadership on a case-by-case basis. This ensures that all business communications are conducted through secure and monitored channels.

Your Texas Baptists email account is intended solely for professional and ministry-related communication. It should not be used for any personal activities, including but not limited to:

- **Financial Matters:** This includes online banking, managing investments, paying bills, or any other activity related to personal finances.
- **Online Shopping:** Your email account should not be used for personal browsing or purchasing of items from online retailers.
- **Insurance:** This includes managing insurance policies, filing claims, or communicating with insurance providers about personal insurance matters.
- **Healthcare:** Your email account should not be used for scheduling appointments, communicating with healthcare providers, or managing personal health information.
- **Newsletters and Subscriptions:** Subscribing to personal newsletters, promotional emails, or other non-work-related content is prohibited.
- **Personal Communication:** While incidental personal communication may occur, the primary use of your email account should be for professional and ministry-related purposes.

Using your Texas Baptists email account for personal activities can lead to security risks, data breaches, and potential misuse of organizational resources. You are responsible for maintaining the confidentiality and security of your email account and for using it in a manner consistent with Texas Baptists' policies and guidelines.

You must exercise caution when interacting with email. Clicking on unexpected or suspicious email, email attachments or links can expose the organization to security threats such as malware or phishing attacks. You should only interact with emails and attachments from trusted sources and you should report any suspicious activity to Texas Baptists IT Help Desk.

Texas Baptists IT reserves the right to remotely delete Texas Baptists data from personal devices that are lost or stolen or when employment ends. This is done to protect sensitive organizational information from unauthorized access.

D. Hardware, Phones, and Mobile devices

You are responsible for ensuring the protection and proper care of assigned Texas Baptists assets. You must promptly report any theft, loss, or damage of Texas Baptists assets to IT.

IT will purchase and install all supported hardware; however, you may use personal peripherals (e.g., keyboards, mice, USB drives, speakers, headsets, microphones, and monitors) if they don't require specialized software, drivers, or IT support.

The Texas Baptists' hardware assigned to you is intended for use solely by you and not by any other individuals, including family, friends, or other persons. Incidental personal use of Texas Baptists hardware, software, and systems is permitted but must be minimal.

When Texas Baptists technology devices are lost or damaged, the cost of replacing the first lost or damaged device or accessory for a given employee will be covered by IT. If that employee loses or damages additional Texas Baptists hardware, then the cost center for the employee must pay for subsequent replacement costs.

Texas Baptists is not responsible for any loss or damage that occurs to personally owned devices, including but not limited to laptops, tablets, smartphones, and other electronic devices, while on Texas Baptists' premises or being used for Texas Baptists-related activities. This includes damage caused by accidents, theft, vandalism, or any other cause. Employees and guests are encouraged to take appropriate precautions to protect their personal devices, such as using strong passwords, installing security software, and backing up data regularly.

Unless Texas Baptists IT authorizes it, you are not allowed to set up wireless networks or access points at Texas Baptists facilities. If the network is down, you may use your personal cell phone as a hotspot only with IT approval.

It is your responsibility to check your voicemail and other messages at least once per day during work hours when you are working. Depending on your manager's specific instructions or the demands of your role, you may need to check your messages more frequently throughout the day to ensure timely responses and stay informed.

You are expected to comply with all applicable laws and regulations regarding the use of wireless communication devices while operating a motor vehicle. This includes, but is not limited to, refraining from texting, emailing, or engaging in other activities that could distract from the road while driving. Hands-free devices may be used where permitted by law, but safety should always be the top priority. In areas where the use of any mobile device while driving is prohibited, employees must pull over to a safe location before using their device.

If you are traveling out of the country for Texas Baptists ministry purposes, you are responsible for adding international calling, data, and text plans to your phones and removing plans after travel is completed. Reimbursement for international plans is subject to your manager’s approval.

E. Prohibited Use

Texas Baptists information resources must be used in a lawful and ethical manner. These resources, which include but are not limited to computer systems, networks, internet access, email, and software, should not be used for any activities that violate local, state, or federal laws. Additionally, these resources should not be used for activities that are prohibited by Texas Baptists policies, such as harassment, discrimination, or the distribution of inappropriate or offensive content.

Prohibited uses include:

- Soliciting, including outside business ventures, products for profit, personal gain, and non-Texas Baptists' fundraising. The sale of personal items internally is an exception.
- Requesting donations outside of normal Texas Baptists processes.
- Making and/or distributing political statements or endorsements outside of normal Texas Baptists assigned responsibilities.
- Making official, legal commitments on behalf of Texas Baptists unless expressly authorized.
- Viewing, downloading, entering, transmitting, or routing of any foul, obscene, profane, offensive, harassing, or otherwise inappropriate messages or material, including gambling. If a user receives this type of material from another party, the user is required to notify his or her supervisor or Human Resources immediately.
- Distributing copies of documents in violation of copyright laws.
- Transmitting messages or jokes that violate Texas Baptists harassment policy or create an intimidating or hostile work environment.
- Sending spam (unwanted communication not specific to all recipients) via any form of electronic communication.
- Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.

F. Confidentiality

To gain access to proprietary information, including but not limited to lists of Texas Baptists churches, all employees and associates must submit a formal request through the Information Management Team (IMT). Any sharing of this information with external parties is strictly prohibited unless explicit approval is granted in advance by Executive Leadership. This policy is in place to safeguard sensitive data and maintain the trust of our constituents.

Furthermore, when traveling with company-issued devices, users are responsible for ensuring the physical and digital security of these devices. This includes, but is not limited to, using strong passwords, and avoiding unsecured Wi-Fi networks. Failure to adequately protect company data while traveling may result in disciplinary action, up to and including termination of employment.

G. Data Ownership and Right to Monitor and Review

Texas Baptists retains full ownership of all data amassed and stored within its systems for the advancement of its ministries. This data encompasses but is not limited to, personal information, communications, and any other data generated through the use of Texas Baptists' systems. Upon termination of a user's relationship with Texas Baptists, whether through resignation, termination, or any

other means, the user relinquishes all rights and claims to this data. Texas Baptists reserves the right to access, monitor, collect, inspect, and divulge any and all information contained within its systems at any time and for any reason deemed necessary, within the bounds of applicable laws and regulations. This may include, but is not limited to, monitoring user activity, reviewing emails and other communications, and disclosing information to law enforcement or other third parties as required by law.

III. Enforcement of this Policy

Violations of this policy may result in disciplinary action, up to and including termination of employment. This applies to all employees of Texas Baptists. In the case of volunteers, contractors, and vendors, a violation of this policy could result in the termination of their current contract or assignment with Texas Baptists. Additionally, legal action may be pursued in cases where the violation involves illegal activities or causes significant harm to Texas Baptists or any related parties.

IV. Supplements to this Policy

This policy will be supplemented by additional Texas Baptists IT Guidelines, which will provide more detailed instructions and procedures for the use of technology resources. These guidelines may cover topics such as acceptable use, data security, password management, software installation, and incident reporting.