1. Purpose:
H-E-B provides various electronic services (depending on need and availability) to our Partners and business associates (also referred to herein as “you” or “users”) or allows the use of certain technology as a productivity tool to assist in the performance of business-related activities.

This guideline governs the use of these electronic services, equipment, and technology administered, facilitated or made accessible by H-E-B, including the following, which will be collectively referred to throughout this guideline as “H-E-B IT”:

(1) H-E-B’s information technology, such as any H-E-B-administered, owned, or leased technology, equipment, computer, or network systems;

(2) email, instant messages, text messages, chat, electronic calendaring, and voice mail, or any other similar technology (collectively, “e-communications”);

(3) social media, including official H-E-B sites on MySpace, Facebook, Flickr, and Twitter (“social media”); and

(4) all electronic services authorized and supported by H-E-B’s Information Solutions (“IS”) Department, all computers attached to H-E-B’s networks, and stand-alone computers with remote access to H-E-B’s networks.

This guideline is designed to protect H-E-B from error, fraud, misuse, alteration, theft, copyright violation, and sabotage, and to protect Partners from unlawful conduct, including discrimination, harassment, and retaliation. It also establishes the default retention practices and periods for certain e-communication transmitted from or received by H-E-B IS servers and confirms roles and responsibilities for implementation, including management of litigation holds. Individual H-E-B departments may maintain their own retention guidelines as required by law or to fulfill business needs or requirements.

This guideline applies to any Partner or other person authorized by H-E-B to use H-E-B IT. All equipment or technology that is owned or provided, facilitated or administered by H-E-B is included within this guideline’s scope. Public access terminals provided by H-E-B are not included in the scope of this guideline, except where those terminals are used by H-E-B Partners to access H-E-B IT.

This guideline does not and is not intended to supersede any local, state or federal laws regarding confidentiality, information dissemination, or standards of conduct, and H-E-B may amend this guideline at any time.

Any violation of this guideline may lead to disciplinary action, up to and including separation of employment and other appropriate legal action.
2. Policy:
   A. Proper Use of Technology
      H-E-B provides access to its technology systems to assist Partners in performing their duties efficiently and effectively. Inappropriate or unauthorized use of information technology exposes H-E-B to internal and external risks and may reduce the effectiveness of those systems. All users of H-E-B IT are responsible for using that technology in an appropriate and lawful manner and in compliance with all H-E-B guidelines, including guidelines prohibiting unlawful workplace harassment, discrimination or retaliation. Any activity performed on a workstation under a Partner’s login ID is presumed to be performed by that Partner and the Partner will be held responsible for any activity.

      Users must be authorized by an appropriate H-E-B manager to use a pager, PDA, home computer, web mail, or a third party service to access their H-E-B e-communication. Users may not use non-H-E-B provided or unauthorized email addresses to receive business related e-communication without the express permission of the Partner’s supervisor.

   B. Privacy and Monitoring/Search
      All files, e-communications, content, data, and other information stored, posted, or transmitted using H-E-B IT are the property of H-E-B, not the user.

      H-E-B reserves the right to, and will routinely, monitor use of H-E-B IT. H-E-B similarly will access or monitor H-E-B social media sites. As a result, and subject to applicable law, there is no expectation of privacy or confidentiality of information maintained, transmitted or stored on H-E-B IT or in the use of any H-E-B IT or official H-E-B social media sites.

      Monitoring of technology usage for personnel-related matters generally requires the approval of the Chief Information Officer and/or the Senior Vice President of Human Resources, or other designated representative.

   C. Acceptable Usage
      H-E-B IT is intended for legitimate H-E-B business only. Users must be careful how they use H-E-B IT, e-communications and H-E-B social media. Inappropriate communications or content may have significant workplace morale issues or legal consequences, such as claims of discrimination, antitrust violation, theft of trade secret, or false advertising. Any software or hardware found on H-E-B IT that has not been approved by IS may be removed, along with associated files, without notice to the Partner. H-E-B social media sites are intended for legitimate business use only. Therefore, only authorized persons may participate on official H-E-B social media sites.
Unacceptable Use: The following are examples of unacceptable or inappropriate use of H-E-B IT and official H-E-B social media sites and are prohibited. The list below is not intended to be exhaustive, but provides a framework for activities which fall into the category of unacceptable use:

- Accessing data which the Partner is not authorized to access or logging into a server or user account that the Partner is not expressly authorized to access;
- Downloading, transferring, or installing software received from an outside source onto H-E-B IT without the approval of IS, including personal software that allows peer-to-peer communications between two workstations (e.g., online chat, Bit Torrent, Kazaa, etc.);
- Adding or removing H-E-B hardware or software, attaching external devices, or making configuration changes to H-E-B IT without approval by IS;
- Using H-E-B IT for personal use, including for e-communications, that interferes with the user’s work performance, negatively impacts the operation of H-E-B or its systems, or results in a material expense to H-E-B;
- Using non-H-E-B managed email systems or communication services (e.g., Yahoo, Google, Hotmail, and Instant Messaging) to conduct H-E-B business without express approval from the Partner’s supervisor. This includes auto-forwarding email from a Partner’s H-E-B assigned mailbox to non-H-E-B managed e-mail systems, including Yahoo, Hotmail, and Google.
- Revealing an H-E-B account password to others or allowing use of an H-E-B account by others. This includes household members and visitors when work is being done at home. Revealing an H-E-B account password to an authorized technician during troubleshooting procedures is not a violation of this guideline. In such a situation, a new password should be established by the Partner as soon as possible after the problem is resolved.
- Creating unnecessary network traffic (e.g. chat room, chain email, playing games, gaming, gambling, chatting on line, non-business media, video or audio streaming, etc.).
- Transmitting, receiving or storing personal audio, video or picture files.
- Causing security breaches or disruptions of H-E-B IT. Security breaches include:
  o intentionally downloading, storing or executing any security, hacking, spyware, keylogger software, or malware tools on H-E-B IT;
  o causing network disruptions including network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for inappropriate purposes;
  o port scanning or security scanning without prior notification to and approval from IS;
  o circumventing user authentication or security of any device, network or account; interfering with or denying service through denial of service attack, or other means;
  o using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, another user's device or session, via any means, locally or via H-E-B’s network; or
SUBJECT: Information Technology and Official H-E-B Social Media Sites – Acceptable Use Guidelines

- Unauthorized reading, deleting, copying or forwarding of electronic communications of another, or accessing electronic files of another without authorization.

- **Inappropriate or Unlawful Material**: Users must not store or transmit material that:
  - is fraudulent, harassing, or otherwise illegal under or violates any local, state, or federal law;
  - violates any H-E-B guideline;
  - is an unauthorized representation of H-E-B, including its trademarks, logos, products, or H-E-B mascot;
  - is sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate, including any material that would offend someone on the basis of race, age, sex, sexual orientation, religion, political beliefs, national origin, veteran status, disability, or other legally protected status;
  - defames H-E-B, its Partners, or business associates;
  - divulges or releases, or causes to be divulged or released, whether intentional or not, sensitive, confidential, or proprietary H-E-B information without the express consent of H-E-B;
  - contains “spam” or otherwise uninvited messages, including junk messages, chain letters, or other mass mailings.

- **Confidential Information**: Carefully consider the confidentiality and sensitivity of any material stored or transmitted using H-E-B IT, e-communications or H-E-B social media. Examples of confidential information include financial information, pricing, cost data, business plans, business strategy, customer information, customer strategy, inventions, software, trade secrets, methods, formulas, product formulations, and personal information of employees, customers, and/or vendors. Portable data storage devices such as jump drives or portable hard drives (e.g., MyBook) should not be used to store or transport H-E-B confidential information without the express consent of the appropriate manager or director. The following guidelines apply to the handling of confidential information in e-communications:
  - Label all confidential communications with “Confidential”. It is recommended that “Confidential” be included in the subject line and in the first line of the e-communication message.
  - Highly sensitive information is best addressed at an in-person meeting.
  - Avoid sending trade secret or other proprietary information through e-communication dissemination.
  - Carefully handle the confidential information of other parties with whom H-E-B does business. H-E-B could be subject to breach of contract or theft of trade secret claims if such information is transmitted without authority.
  - If the e-communication is to an H-E-B in-house attorney or outside legal counsel, identify it as “Confidential Attorney/Client Communication”. It is recommended that this language be included in the subject line and on the first line of the e-communication message.
Avoid transmitting personally identifiable information or personal health information of H-E-B employees, customers or vendors (e.g. social security numbers, drivers license numbers or prescription information, credit or debit card account numbers) through an e-communication unless in accordance with applicable privacy laws and H-E-B guidelines.

Protected Intellectual Property: Do not store or transmit any material that violates any copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including by installation or distribution of "pirated" or other software products that are not appropriately licensed for use by H-E-B.

Contracts. When communicating via e-communication with a customer, vendor or other business partner, be careful not to make statements or acknowledgements that could inadvertently result in binding H-E-B to an agreement or modify an existing agreement.

Competition/Antitrust. E-communications about pricing and competition should be drafted carefully. Although a pricing program may be implemented with no anticompetitive purpose or intent, carelessly worded documents or communications (including emails, drafts of documents or other purely internal communications among H-E-B personnel) may be mischaracterized to suggest a violation of antitrust laws.

D. General E-communication Best Practices
All e-communications should be drafted carefully. Because e-communication can be inadvertently sent to incorrect or unintended recipients or intercepted or obtained by third parties, users should assume all e-communications will be read by others. Improperly worded or inappropriate e-communication could harm H-E-B’s reputation, our Partners or the community. The following lists some general guidelines to follow when sending e-communications.

Recipients: Double-check the recipients. Do not inadvertently “reply to all”. Verify the auto-population of the recipient lines.

Copies: Provide copies only to recipients who have a need to know the information in the email.

Priority: Do not mark an email as high priority unless it truly is important.

Etiquette: Be respectful in drafting. Nuances and inflections that may be detected in person do not always transmit via e-communication. Do not curse or name call.

Solicitations; marketing; spam: Do not send unsolicited advertising or marketing e-communication.

Confirm Delivery: For important e-communication, confirm through other means, such as a telephone call, that the email has been received.
E. **Email and Electronic Calendaring Security**

Email and calendar attachments containing unsafe file types will be removed from e-mail messages passing through H-E-B’s central mail servers. This system will employ content filtering as a technical measure to ensure message integrity, confidentiality, and system availability.

E-mail and calendar attachments are scanned for virus content. Removed attachments are replaced by a message indicating that they have been removed and the header and text of the original message delivered normally.

In many cases, a spam message filter will be implemented to prohibit the transmission of chain letters, broadcast announcements, general advertisement postings, or any other message via email to a group of persons not requesting the message except when conducting official H-E-B business.

Encryption of e-communications containing confidential or proprietary information is required.

F. **Email Signatures**

We understand that on occasion, personal, non-business related email may be transmitted using H-E-B IT. However, great care should be taken to avoid communication from being interpreted as official H-E-B material or opinion, and there is no expectation of privacy. As a result, personal emails must comply with this guideline and should include a footer as follows:

“This message is a personal communication prepared by and intended solely for the use of the author. Statements, representations, and material omissions contained within this message are not binding upon H-E-B, its subsidiaries, affiliates, or any entity other than the author."

If the content of an email contains sensitive or confidential information, include a footer as follows:

“This message contains information which may be confidential and privileged. Unless you are the addressee (or authorized to receive for the addressee), you may not use, copy or disclose to anyone the message or any information contained in the message. If you have received the message in error, please notify the sender and delete the message immediately."

G. **Email Calendaring**

Calendar objects should provide only essential logistical information. Attachments and general messaging within the body of the calendar event are prohibited and should only be used when alternative communications are not available or reasonable. It is advised that you use personal calendar events as place holders and not include any descriptive language the user would not intend to become public knowledge.
H. Email Retention
Read and unread email located in a user’s mailbox will be deleted ninety (90) days from receipt.

Due to space and cost considerations, H-E-B email systems will be configured to allow users to selectively archive email messages. Users will be allocated a fixed size archive folder to which they may save messages. The quota will be applied as a standard for all H-E-B mailboxes. Archive folders should be used to store business-related communications in a manner consistent with the appropriate retention schedules.

Any email that has been deleted automatically from the user’s Mailbox or from the archive cannot be restored.

Mailboxes of departed Partners or contractors of H-E-B will be de-provisioned immediately upon the end of contractual relationship or employment and deleted 30 days from account termination. Once deleted, mailboxes cannot be restored.

Email messages maintained by a user in violation of this guideline may be automatically deleted by authorized personnel without advance warning. Users should not circumvent storage prohibitions by sending, forwarding, or copying any email messages or related documents to themselves or others for the purpose of evading this requirement. Users are responsible for managing all email synchronized to external sources (e.g., mobile phones) in accordance with this guideline.

I. Email Backup Files
Backup copies of H-E-B email system files will be kept for no more than 28 days. These backups are for system restoration and disaster recovery purposes, and are not designed to facilitate retrieval of deleted messages. Users are prohibited from making backup copies of email items or their mailbox.

J. Personal Archives and Personal Storage Files (PSTs)
The usage of “offline” personal archives and personal storage files is prohibited unless approved by H-E-B’s General Counsel or Chief Information Officer. If approved, e-communications stored in a personal archive or PST must be stored on H-E-B’s networked servers, and not on computer hard drives, local drives, CD-ROMs, flash drives, thumb drives or other removable media. Names of sender, recipient, date/time of the message, as well as any attachments must be retained with the message if approved for using a personal archive or PST.

K. Litigation Holds
In certain cases, the law imposes a duty upon H-E-B to preserve all documents and records, especially when it relates to litigation or governmental investigations (“litigation hold”). A litigation hold directive is typically issued to the legal custodians of those documents. Partners who receive a litigation hold directive may not alter or delete an electronic record that falls within
the scope of that hold. In addition, Partners are required to provide access to or copies of any
electronic records that they have downloaded and saved, or moved to any other storage account or
device. E-communications and accounts of separated Partners that have been placed on litigation
hold status must be maintained by IS until the hold is released.

A litigation hold directive overrides this e-communication guideline, as well as any records
retention schedules that may have otherwise called for the transfer or retention limits of relevant
documents until the hold has been cleared.

L. Instant Messaging Retention
H-E-B IT does not store instant messages.

M. Voice Mail Retention
H-E-B does not support the conversion of voice mail messaging to e-communication for
corporate devices and services. H-E-B voice mail systems do not retain voice mails in an
attendant after 60 days.

3. Responsibilities:
A. Information Solutions (IS)
1. IS has organizational responsibility for establishing, communicating, maintaining, and
   compliance monitoring of requirements established in this guideline.
2. IS may disconnect e-communication, network, and Internet services to any user or computer
   at any time should connectivity constitute a threat to H-E-B or H-E-B IT, business services,
   or be a violation of this guideline. IS will attempt to contact the person responsible for the
   computer prior to disconnecting as long as such notification does not allow further
degradation of H-E-B-administered technology or equipment. Such notification will be made
   after the disconnection if prior coordination was not possible.
3. Where appropriate, IS will provide technology solutions to enforce the terms of the guideline
   and to ensure compliance with corporate retention guidelines.

B. Users
1. Each user is responsible for ensuring that his/her use of H-E-B IT is consistent with this
guideline and the retention guideline for your department as well as procedures of ethical
conduct, safety, compliance with applicable laws, and proper business purposes.
2. It is the responsibility of the user of the e-communication system to manage e-communication
   messages according to H-E-B’s approved retention periods. The same applies to messages
   that relate to H-E-B business that are sent from or received on non-H-E-B owned computers.
3. Except for appropriate, business-related listserv mailing services, distribution lists must be
   able to identify the sender and recipient of the message.
4. Users who voluntarily separate from H-E-B, retire, or are transferred, will be required to
   review their email account with their supervisor or other appropriate IS Partner. The user’s
   supervisor is responsible for ensuring the email records are properly classified, stored, and
   that working or convenience copies are disposed of in the prescribed manner.
5. Email accounts for separated Partners or users will be the responsibility of the user’s supervisor. The user’s supervisor is responsible for ensuring the email records are properly classified, stored, and that working or convenience copies are disposed of in the prescribed manner.

C. Reporting Responsibilities

Any violation or suspected violation of this policy must be reported immediately, or as soon as practicable, to the IS Department or the H-E-B Compliance and Ethics Helpline (866-208-8167 or https://www.tnwgrc.com/hebcompliancehelpline/).
ACKNOWLEDGEMENT

I have received a copy of H-E-B’s Guideline 5.6 - Information Technology and Official H-E-B Social Media Sites – Acceptable Use Guidelines. I have read and understood the Guideline and agree to abide by its terms. I understand that failure to follow the Guideline is a violation of Company policy and may lead to appropriate disciplinary action, up to and including separation of employment.

____________________________________________________________________________
Partner Signature                                               Date

____________________________________________________________________________
PeopleSoft Employee ID#                                           Store # or Corporate Location