# TECHNOLOGY and ADMINSTRATION POLICY

## INTRODUCTION

This policy provides guidance on Chapter administration, including the administration and use of technology-related services which may be provided to ACFE-GTA Chapter Officers, to certain directors for Chapter functions (e.g., website, membership), as well as to third-party contractors (e.g., the Chapter Administrator, etc.). These parties are herein referred to as "**those associated with the ACFE-GTA Chapter**".

Access to technology-related services (e.g., email, internet access, third-party supplied services, Chapter Administration section of ACFE website, the ACFE-GTA Chapter website, etc.) may be provided to those associated with the ACFE-GTA Chapter for Chapter business-related activities **only**.

Technology access by those associated with the ACFE-GTA Chapter may be through a personal or ACFE-GTA Chapter-provided personal computer or laptop, or a personal or ACFE-GTA Chapter-provided mobile device. At all times, this access must be used and managed in a responsible manner and in accordance with the ACFE Code of Professional Ethics, this Policy, and any applicable policy or legislation.

## PRINCIPLES

### 1. Appropriate Use

a) Email access is provided by ACFE-GTA Chapter through a third-party supplier to facilitate ACFE-GTA Chapter business communications only.

b) ACFE-GTA Chapter email services are **not** to be used for personal communications.

c) To support the reputation of the ACFE-GTA Chapter and ensure authenticity of messages, those associated with the ACFE-GTA Chapter **are required** to use the assigned ACFE-GTA Chapter email address for all ACFE-GTA Chapter business and communications.

d) Those who receive personal emails to an ACFE-GTA Chapter account are advised to re-direct the messages to a personal account, and to ask the sender to use their personal account in the future.

### 2. Privacy and Ownership

a) **Email activity** on ACFE-GTA Chapter email accounts **is monitored on a regular basis** by the Executive Vice-President (EVP), who acts as both the Chief Technology Officer and Chief Compliance Officer, or a director designated by the Executive Vice-President.

b) Users should have **NO** expectation of privacy regarding email messages they create, respond to, or receive using ACFE-GTA Chapter resources.

c) Information created using Chapter resources, including email, is considered Chapter property.

3. **Security of ACFE-GTA Chapter Materiel**

a) Those associated with the ACFE-GTA Chapter have an obligation to protect ACFE-GTA Chapter information and the integrity of ACFE-GTA Chapter assets, infrastructure, and resources.

b) Those associated with an ACFE-GTA Chapter email account are expected to use common sense, good judgment, and proper security when using email and other technology services, as they are responsible for any all communications and actions completed using their logon ID.

c) The following activities are **not permitted** as they represent a security risk, can negatively impact shared technology resources and performance for all users, and have the potential to cause reputational risk or additional expense to the ACFE-GTA Chapter:

i. Creating or distributing messages with large distribution lists or attachments. All notices to members are to be sent from the ACFE-GTA Chapter website using the Wild Apricot services or from the Mailchimp or other such service as determined.

ii. Forwarding content from personal email messages and storing them on ACFE-GTA Chapter email accounts (e.g., chain letters, junk mail, advertisements, executable graphics, personal photos, music, etc.)

iii. Divulging, sharing, or compromising your ACFE-GTA Chapter authentication credentials with other authorized or unauthorized users.

iv. Sending ACFE-GTA Chapter related emails (including those that contain any electronic attachments, files, documents, etc.) to a personal email account or to an unauthorized person's email account.

v. Conducting illegal activities.

vi. Sending messages and/or attachments that contain racist, sexist, or sexually explicit items or content including pictures, jokes, hoaxes, or executable graphics.

vii. Sending hate mail, harassing others, making discriminatory remarks, or using objectionable language.

viii. Misrepresenting others associated with the ACFE-GTA Chapter by sending email from another ACFE-GTA Chapter user's account.

ix. Conducting or pursuing business interests other than those of the ACFE-GTA Chapter, including their own or those of another organization.

i. Political lobbying.

d) Technical support for the ACFE-GTA Chapter, including passwords for ACFE-GTA Chapter email accounts and access to the ACFE-GTA Chapter website administrator log-in, is provided by the Executive Vice-President (EVP), who acts as the Chief Technology Officer and Chief Compliance Officer of the Chapter, or by a director designated by the EVP.

Access and password requirements include:

i. All passwords and access instructions are to be provided in a confidential and/or password-protected manner.

ii. All requests for password change are to be made to the Executive Vice-President or designate.

iii. All password holders are to exercise a high level of security, including:

1. Keeping their password secure and not sharing it with anyone else;
2. If permitted to determine their own password, selecting strong passwords that can't be guessed by third parties;
3. Using Two-Factor Authentication or Verification where available.

e) While most business, government, or organizational offices maintain strong security WiFi access standards, those associated with the ACFE-GTA Chapter who have been granted email or website access must ensure proper security procedures are in place at their point of access (e.g., their home, or cottage, etc.) as follows:

i. **WPA2 Personal (AES)** is currently the strongest form of security offered by Wi-Fi products, and is recommended for all uses.

ii. If you have older Wi-Fi devices that don't support WPA2 Personal (AES), a good second choice is **WPA/WPA2 Mode**, also known as WPA Mixed Mode. This mode allows newer devices to use the stronger WPA2 AES encryption, while still allowing older devices to connect with older WPA TKIP-level encryption.

iii. If your Wi-Fi router doesn't support WPA/WPA2 Mode, **WPA Personal (TKIP)** mode is the next best choice. For compatibility, reliability, performance, and security reasons, the **WEP router setting is <u>not</u> recommended**.

iv. Never accessing ACFE-GTA Chapter-related accounts using **public WiFi** (e.g., in a coffee shop or retail outlet) **without using a paid (not free) accredited VPN**

f) Under the guidance of the Executive Vice-President and with the assistance of the Chapter Administrator, all those associated with the ACFE-GTA Chapter must ensure **proper and regular backup of all ACFE-GTA Chapter digital materials** in their safekeeping, including but not limited to bookkeeping and accounting program files, policies and procedures, website pages, electronic communications, etc.

# TECHNOLOGY and ADMINSTRATION POLICY

**PROTECTION of PERSONAL INFORMATION**

As of January 1, 2004, the Federal Personal Information Protection and Electronic Documents Act (PIPEDA) applies to most organizations in Canada, including our ACFE-GTA Chapter. This legislation controls how organizations collect, store, use, and disclose personal information about individuals in the course of providing services to “members.”

In our circumstances, a “member” is defined as an active or lapsed member of the ACFE-GTA Chapter **or** Certified Fraud Examiners and Associate Members of the Association of Certified Fraud Examiners, ("ACFE" with World Headquarters in Austin, TX, USA) who are **not** members of the GTA Chapter.

Members provide the ACFE-GTA Chapter and/or the ACFE (Austin, TX) with personal information to provide them a service and to communicate with them in a timely manner. ACFE (Austin) allows the ACFE-GTA Chapter access to some of this information. All personal information contained in the ACFE-GTA Chapter files, lists, and on the ACFE-GTA Chapter website, as well as on the ACFE website (under the “Chapter Administration” section), are the property of the ACFE-GTA Chapter or the ACFE respectively, and are prohibited from being used for any purpose **other** than Chapter business.

All Board members, employees, volunteers, and third parties who are granted access to this member and non-member personal information are to sign, at the beginning of their term of office, and periodically from time to time as determined by the President or the Board of Directors, an acknowledgement of their understanding of the legal requirement to keep this information protected and confidential, and that the use the information only is for ACFE-GTA Chapter business only.

**VIOLATIONS of this POLICY**

Those associated with the ACFE-GTA Chapter who violate this policy may be subject to disciplinary action up to and including termination of association, membership, contractual arrangements and employment with the ACFE-GTA Chapter, as well as potential referral to the relevant law enforcement agency, as appropriate.

**APPROVAL and IMPLEMENTATION**

This policy has been approved by the ACFE-GTA Chapter Board of Directors on September 9, 2019 and comes into effect immediately. Questions about the application of this Policy can be directed to the President or the Executive Vice-President and Chapter Chief Compliance Officer.