WILLIAMSON
COLLEGE of the TRADES
Founded 1888

April 5, 2018

Office of the Senior Vice President/Chief of Staff

Policy Letter: Safeguarding Confidential Information

This document provides recommendations for the implementation of administrative, technical, and physical safeguards designed to:

- Ensure the security of any confidential information in the College's custody in all forms, no matter if that information is contained electronically, written, or in any other format.
- Protect confidential information against any threats or hazards of integrity, unauthorized access, or unauthorized use.

Definitions

Confidential Information

Confidential Information means any information not exempted in specific legislation and identified as personal, sensitive, or confidential such as personally-identifiable information, individually-identifiable health information, education records, and non-public information as specified in all applicable federal or state laws, plus Williamson College policies. Confidential information includes, but is not limited to, the following examples:

- Social Security number
- Physical description
- Home address
- Home telephone number
- Ethnicity
- Gender
- Education (except student records which are exempted by FERPA)
- Financial matters
- Performance evaluations
- Verbal or written statements made by or attributed to the individual
- Medical and employment history
- Social Security number
- Driver's license number
- Account number, e.g., identification number, credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Confidential information may include individually-identifiable health information. This includes any information, including demographic information collected from an individual, created or received by a health care provider, health plan, employer, or health care clearinghouse. This includes information that relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to the individual, or the identification of the individual.

In addition, electronic confidential information is defined as any electronic format which includes an individual's first name or first initial and last name or education in combination with any one or more of the following data elements, when either the individual's name or the data elements are not encrypted:

- Social Security number
- Driver's license number
- Account number, e.g., identification number, credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Unauthorized Disclosure

Unauthorized Disclosure means to disclose, release, transfer, disseminate, or otherwise communicate all or any part of any record orally, in writing, or by electronic or any other means to any person or entity.

College Practices in Safeguarding Confidential Information

All confidential information must be cared for with the appropriate level of physical and electronic (logical) security. When working with confidential information the College takes on the custodial responsibilities for that information. Thus each person who access this information also has the responsibility to:

- **Identify**
- **Protect**
- **Communicate**
- **Maintain**

These terms are defined below. Note: These lists are not exhaustive. Each of them are provided to serve as included examples. As technology develops, each of these lists should be expanded to cover additional techniques and devices as appropriate

Identify

Identify and inventory where confidential information is stored, processed, or transmitted. Here are some examples:

Confidential information

- E-mails
- Electronic documents
- Printed information (paper)

Computer information systems

- Desktop computers
- Laptops / notebook computers
- Mobile devices

Local storage device

- Hard drive
- Internal memory sticks/cards

Removable media

- External hard drives
- CD or DVD (optical)
- USB-devices

Remote storage device

- Shared/mapped drive
- Network Attached Storage (NAS)
- Storage Attached Network (SAN)

Protect

Protect confidential information against unauthorized access, unauthorized use, loss, or damage. The College maintains a custodial partnership with each individual who accesses its network. Specific policies and procedures in exercising this partnership is the responsibility of the both the institution and individual to include

- Individual: Do not share or disclose personal authentication credentials, such as user-ids and passwords or other forms of electronic authentication with other individuals.
- Individual: Do not use personal credentials for authentication to provide other individuals with access to any information systems containing confidential information.
- The College: Maintain up to date and install all appropriate security software updates in all computer workstations and laptops and software applications
- The College: Install and maintain antivirus software in all computer workstations and laptops and set them to auto-update to install the latest antivirus signatures.
- The College and Individual: Keep portable equipment and storage devices such as CD, DVD, USB drives, or other removable storage media in an appropriately access limited location.
- The Individual: Do not leave computer equipment or portable storage devices unattended.
- The College: Use boot-up (BIOS) passwords for appropriate computer systems and set strong authentication for all user accounts, including any accounts with administrative rights.
- The College: Enable screen savers with authentication (Locking passwords) for all computer systems.
- The Individual: Use caution when accessing e-mail, and do not trust any unexpected e-mails. Never open an attachment without first verifying its type and checking it with an antivirus program. If in doubt, delete it, and/or contact the sender first.
- The Individual: Position monitors and printers so that others cannot see or obtain confidential or sensitive data.
- The Individual: Log out, shut down, or lock the system when leaving your computer unattended at any time.

- The College: Physical safeguards (keys, cipher locks, passwords, etc.) which are used to secure confidential information are changed regularly, including every time someone who formerly had authorized access either leaves college employment, no longer has job requirements which require access, or a key securing such access is lost, stolen or unaccounted for.

Communicate

Individual accessing the College's network have a responsibility to communicate with care to include:

- Promptly reporting any possible unauthorized access, use or loss of information or an information system to your immediate supervisor.
- Never send confidential information using non-secure applications such as IM, Chat programs or regular e-mail.
- Never send sensitive information to e-mail accounts other than on-campus accounts. Use an authenticated method of distribution when on-campus accounts are not available.
- Always use an authenticated and approved protocol for remote communication when accessing critical servers or resources containing personal or confidential information. Use the campus VPN when accessing any critical servers such as CMS or SIS from off campus.
- Get appropriate authorization before taking College equipment off-site.

Maintain

The College and Individual must work in partnership to:

- Maintain confidentiality, integrity, and access measures up-to-date.
- Securely dispose of unnecessary confidential information in an approved manner.
- Remove any confidential and private information that it is no longer needed. This will minimize the liability in case the computer becomes infected or compromised.
- Ensure that confidential, sensitive, or personal data is properly cleansed from internal disks or removable media prior to disposal or transfer to others. Seek authoritative advice on disposing of equipment and data.

If you have any questions regarding this letter, please contact the Senior Vice President/Chief of Staff

//Signed//
Senior Vice President/Chief of Staff