4.6 - Information Technology - Policy

Section: Operations
Subject: Information Technology
Policy: 4.6
Approved: November 20, 2001
Reviewed: May 21, 2013
Revised: December 15, 2015

Carlton Trail College will maintain an up-to-date Procedure Manual which provides direction for the use and management of IT resources within the College, and which must be followed by all staff and members of the College community.

Carlton Trail College will notify employees when a significant change in a policy or procedure has been made.

4.6.1 - Hardware Purchase - Procedure

Section: Operations
Subject: Hardware Purchase
Procedure: 4.6.1
Approved: December 15, 2015

Objective

To provide guidelines for the purchase of hardware for Carlton Trail College to ensure that all hardware technology for the College is appropriate, cost effective and where applicable, integrates with other technology for the College. The objective of this procedure is to ensure that there is minimum diversity of hardware within the College.

Procedures

Purchase of Hardware

- The purchase of all desktops, servers, portable computers and computer peripherals must adhere to this procedure.
- Portable computer systems include notebooks, laptops, tablets etc.

Purchasing Computer Systems

- Computer systems purchased must run a Windows 7 Professional Edition or newer and integrate with existing hardware in the College.
- The portable computer systems purchased must be from a reputable manufacturer.
- The College currently uses Lenovo, Dell and Acer brand computers.

The minimum capacity of the portable computer system, excluding tablets, must be:

- Intel Core i3-3230M CPU @ 2.60GHz
- 4.00 GB Installed Memory (RAM)
- 3 USB ports
- Specifications for devices, such as DVD drive, microphone port, webcam, speakers, etc. is dependent on the manufacturer bundle purchase.

The portable computer system must at least include the following software provided:

- Internet Explorer
- Microsoft Office Professional Plus 2010 or higher
- Adobe Reader XI or higher
- Adobe Flash Player 18 Active X
- Microsoft Security Essentials
- Microsoft Visual Studio 2010 Tools for Office Runtime
- Firefox

Other staff may have one or all of the following programs installed on their computers depending on their job functions:

- Easy Grade Pro Plugin
- Smart Notebook(Collaborating Learning Software 2013)
- OCSM (One Client Student Management)
- Adobe Connect 9 Add-in
- Microsoft Dynamics NAV 2013
- Grand Master Suite version. 7.01
- Live Link web

Any change from the above requirements must be authorized by the IT department.

All purchases of all portable computer systems must be supported by guarantee and/or warranty requirements and be compatible with the College's server system.

Purchasing Server Systems

- Server systems can only be purchased by the Information Technologist with the approval of the VP Finance.

- Server systems purchased must be compatible with all other computer hardware in the College.
- All purchases of server systems must be supported by guarantee and/or warranty and be compatible with the College's other server systems.
- Any change from the above requirements must be authorized by the VP Finance.

Purchasing Computer Peripherals

- Computer system peripherals include printers, scanners, external hard drives, etc.
- Computer peripherals can only be purchased where they are not included in any hardware purchase or are considered to be an additional requirement to existing peripherals.
- Computer peripherals purchased must be compatible with all other computer hardware and software in the College.
- The purchase of computer peripherals can only be authorized by the employee's manager in coordination with the IT department.
- All purchases of computer peripherals must be supported by guarantee and/or warranty and be compatible with the College's other hardware and software systems.
- Any change from the above requirements must be authorized by the IT department.

4.6.2 - Equipment Requests - Procedure

Section: Operations
Subject: Equipment Requests
Procedure: 4.6.2
Approved: December 15, 2015

Objective

To provide employee guidelines for ordering new technology equipment or making changes to existing equipment in order to streamline the order process and to assist the IT staff in fulfilling the request.

General

- All technology equipment requests are reviewed and approved by the Manager or VP in charge of the employee making the request, the IT Systems Support and the VP Finance for appropriate need.
- All employees may submit equipment requests.

- Response times for various new equipment installations, changes, etc. depend on the type of device or equipment being requested and its availability.
- Appropriate lead time should be taken into consideration when ordering new equipment, upgrades, equipment relocations, etc. The wait time for small equipment or devices like mouse or a thumb drive, is at least three work days and for bigger equipment purchases, like a PC is at least two to three weeks.
- The IT Systems Support will maintain a small inventory of standard PC's and other heavily used equipment to minimize the delay in fulfilling critical orders.
- It is the IT Systems Support's responsibility to provide enough lead time for new orders and change requests in order to manage equipment requests effectively.

Procedure

1. Communicate to your Manager or VP the equipment that you need for review and approval prior to submission.

2. Submit the request to the IT Systems Support through helpdesk for review and follow-up.

3. The IT Systems Support will review the request for appropriateness and will follow-up in one of the following ways:

- Purchase Order is filled out, if the equipment requested is not in the inventory, and is forwarded to the VP Finance for approval.
- Fill the order if equipment is available in inventory.
- Contact the requesting employee for notification and/or clarification.
- Decline the request with an explanation back to the originating employee through Help Desk.

Approved Equipment

- If the equipment exists in inventory, the equipment is prepared as needed and installed for the requesting employee.
- If the equipment is ordered, expect a wait time of two to three weeks. Once the equipment has been received; the requesting employee will be notified by the IT staff and the equipment will be prepared and installed.

4.6.3 - Software Purchase - Procedure

Section: Operations
Subject: Software Purchase
Procedure: 4.6.3
Approved: December 15, 2015

Objective

To provide guidelines for the purchase of software for Carlton Trail College to ensure that all software used by the College is appropriate, cost effective and where applicable, integrates with other technology for the College. This procedure applies to software obtained as part of hardware bundle or pre-loaded software.

Procedures

Request for Software

All software, whether commercial or freeware must be approved by the employee's manager and depending on the usage, by the Information Technologist or Educational Technologist prior to the use or download of such software. As a matter of practice, software should always be demoed prior to purchase.

Purchase of Software

The purchase of all software must adhere to this procedure.

Upon approval from the Executive Team, software used for operations is to be purchased by the Information Technologist, whereas software used for educational purposes is to be purchased by the Educational Technologist.

All software must be purchased from reputable software sellers.

All purchases of software must be supported by guarantee and/or warranty and be compatible with the College's server and/or hardware system.

Where possible taking advantage of Provincial licensing is encouraged.

Obtaining Open Source or Freeware Software

Open source or freeware software can be obtained without payment and usually downloaded directly from the internet.

In the event that open source or freeware software is required, approval from the Information Technologist for software use in operations or Educational Technologist for software use in education must be obtained prior to the download or use of such software.

All open source or freeware must be compatible with the College's hardware and software systems.

4.6.4 - Software Installation - Procedure

Section: Operations
Subject: Software Installation
Procedure: 4.6.4
Approved: December 15, 2015

Objective

To provide guidelines on the proper installation of software on Carlton Trail College's computing devices to minimize the risk of lost program functionality; the exposure of sensitive information contained within the College's computing network, the risk of introducing malware and the legal exposure of running unlicensed software.

Scope

This procedure covers all computers, servers, smartphones and other computing devices owned by Carlton Trail College.

Procedure

- Employees may not install software on Carlton Trail College's computing devices operated within the College's network.
- Software requests must first be approved by the requester's supervisor and then be made to the Information Technology department through the Help Desk in writing or via email.
- Software must be selected from an approved software list, maintained by the IT staff, unless no selection on the list meets the requester's need. The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.
- Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., IT support staff may have a need to install software for evaluation purposes for the legitimate future use of the college.)

Breach of Procedure

- Any employee found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment.

4.6.5 - Software Usage - Procedure

Section: Operations
Subject: Software Usage
Procedure: 4.6.5
Approved: December 15, 2015

Objective

To provide guidelines for the use of software for all employees within Carlton Trail College to ensure that all software use is appropriate. Under this procedure, the use of all open source and freeware software will be conducted under the same guidelines outlined for commercial software.

Procedures

Software Licensing

- All computer software copyrights and terms of all software licenses will be followed by all employees of the College.
- Where licensing states limited usage (i.e., number of computers or users etc.), then it is the responsibility of the IT staff to ensure these terms are followed.
- The Educational Technologist is responsible for completing an audit of all software twice a year to ensure that software copyrights and license agreements are adhered to.

Software Installation

- All software must be appropriately registered with the supplier where this is a requirement.
- Carlton Trail College is to be the registered owner of all software.
- Only software obtained in accordance with the Software Purchase Procedure is to be installed on the College's computers.
- All software installation is to be carried out by IT staff.

Software Usage

- Only software purchased in accordance with the Software Purchase Procedure is to be used within the College.
- Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.
- Employees are prohibited from bringing software from home and loading it onto the College's computer hardware.
- Unless express approval from an employee's manager is obtained and based on the job requirement of an employee, software cannot be taken home and loaded on an employees' home computer.
- Where an employee is required to use software at home, an evaluation of providing the employee with a portable computer should be undertaken in the first instance. Where it is found that software can be used on the employee's home computer, authorization from his/her manager is required to purchase separate software if licensing or copyright restrictions apply. Where software is purchased in this circumstance, it remains the property of the College and must be recorded on the software register by the IT staff.
- Unauthorized software is prohibited from being used in the College. This includes the use of software owned by an employee and used within the College.
- The unauthorized duplicating, acquiring or use of software copies is prohibited. Any employee, who makes, acquires, or uses unauthorized copies of software will be referred to the VP Administration for further consultation or reprimand. The illegal duplication of software or other copyrighted works is not condoned within the College and the VP Administration is authorized to undertake disciplinary action where such events occur.

Breach of Procedure

- Where there is a breach of this procedure by an employee, that employee will be referred to the VP Administration for further consultation or reprimand.

4.6.6 - Information Technology Use and Management - Procedure

Section: Operations
Subject: Information Technology Use and Management
Procedure: 4.6.6
Approved: December 15, 2015

Objective

To define the College's expectations and requirements for the use and management of the College information technology resources.

Procedure

Information technology resources should be used primarily for activities related to the mission of the College, including, but not limited to teaching, learning, research and administration. Limited personal use (i.e., use not related to the mission of the College) is permitted provided it complies with this procedure, does not compromise the business of the College, does not increase the College's costs, does not expose the College to additional risk, does not damage the College's reputation, and does not unduly impact the College's business and academic uses. All other uses are prohibited.

Information Technology resources must be used and managed in a responsible manner. Use of these resources for disruptive, fraudulent, harassing, threatening, obscene (including but not limited to racist, profane, and pornographic in nature), or malicious purposes is strictly prohibited. Use of information technology resources for commercial purposes is prohibited unless authorized by the appropriate supervisor or VP.

Application and enforcement of this procedure shall not in any way, constrain academic freedom in the College provided technology resources are used for activities outlined in point #1.

Use of College information technology resources, including electronic identities, is permitted only to members of the College community, and authorized guests.

Information technology resource users must stay within their authorized limits and refrain from seeking to gain unauthorized access to information technology resources beyond their permissions and privileges.

Any individual using information technology resources to create, access, transmit or receive College-related information must protect that information in a manner that is commensurate with its value, use, and sensitivity.

Users must respect the rights of other users. They must not intrude on other users' rights to use, access, and privacy within the employer/employee relationship.

All forms of electronic communication are expected to reflect high ethical standards and mutual respect and civility. Users must refrain from transmitting to others, inappropriate images, sounds, or messages which might reasonably be considered harassing, fraudulent, threatening, obscene (e.g., pornographic), defamatory, or other messages or material that are a violation of applicable law or College procedure.

Users must be sensitive to the open nature of public spaces (for example, computer labs and classrooms) and ensure that they do no create, transmit or display any images, sounds or messages that may be loud, harassing, threatening, obscene (e.g. pornographic), defamatory, or that are in violation of College procedure.

Users must respect intellectual property, copyrights, and licenses to software, entertainment materials, published and unpublished documents, and any other legally protected digital information.

The College will protect information against unauthorized disclosure. The College reserves the right to access, monitor and record both stored or in-transit data and the usage of information technology resources when there is suspected or alleged impropriety, a business need for access in the absence of an employee, a request under the Local Authority Freedom of Information and Protection of Privacy Act, or as otherwise required by law. The College has the right to use information gained in this way in disciplinary actions and to provide such information to appropriate internal and external investigative authorities.

Anyone witnessing unacceptable use of College information technology resources in a manner that contravenes this procedure, or suspects an information technology security incident, is obligated to report it to a member of Executive Team.

The College reserves the right to withhold and revoke access to its information technology resources to any individual if there are reasonable grounds to suspect that their continued access to the resources poses a threat to the operation of the resource or the reputation of the College.

System administrators of information technology resources have the responsibility to investigate and take action in the case of suspected or alleged unacceptable use. With the approval of a member of the Executive Team and with due regard for the rights of users' privacy and the confidentiality of users' data, system administrators have the right to suspend or modify users' access privileges to information technology resources. System administrators have the responsibility to take immediate action in the event the College is an imminent risk. Upon approval from the Executive Team, system administrators may examine files, passwords, accounting information, data, and other material that may aid in an investigation of possible abuse.

Breach of Procedure

- Non-compliance with this procedure constitutes misconduct and may be handled under the applicable collective agreements, College procedure, or law.

4.6.7 - IT Asset Management - Procedure

Section: Operations
Subject: IT Asset Management
Procedure: 4.6.7
Approved: December 15, 2015

Objective

To provide rules and guidelines for managing the use, inventory and reporting of IT assets at Carlton Trail College.

General

PCs, equipment, and supplies are purchased for College employee use and productivity. It is the responsibility of all employees, upon approval from their supervisor to coordinate with IT staff regarding requests, changes and acquisition of IT equipment. It is the IT staff's responsibility to manage the inventory of College equipment and supplies in order to cost effectively manage the college's expense in these areas.

Procedures

Allocating Equipment to Employees

- Equipment is assigned to employees based upon their job function.
- IT staff should maintain a list of equipment allocated to each employee.
- Specific equipment should be tracked by IT staff which includes, but is not limited to:
    - PC's (both desktop and laptop)
    - PC peripherals (keyboards, monitors, scanners, printers, fax machines, mouse, headset, etc.)
    - Audio-visual equipment such as Smartboards, projectors, etc.
    - Headphones and headsets
- All equipment should be used for work purposes only.
- Any equipment purchased by the College remains the property of the College.

Movement of Equipment

- Employees should inform IT staff regarding transfer of equipment from one location to another. IT staff will then update the inventory report with the current equipment location. This allows easy tracking and accountability of moved items.

Missing Items/Equipment

- Any missing item/equipment should be reported by employees to the IT staff. The IT staff will conduct a search for the said item/equipment. Missing items not found within a year will be deleted from the inventory. If the missing item/equipment is found, the inventory report should be updated. Both missing and found items/equipment should be reported by the IT staff to the VP Finance.

Employee Termination

- For transfer or termination of employment, it is the responsibility of IT staff to conduct a physical inventory of IT equipment to check against the inventory record.
- Upon approval from the VP Finance and VP Administration, employees who are not able to return allocated equipment will be responsible for reimbursing the College for the fair market value of the item(s).

Technology Assets

IT staff will maintain an accurate inventory of all Information Technology assets. IT staff will tag the item/equipment as soon as it is received. The following information should be included in each tag:

- Item
- Serial #
- Basic configuration (i.e., Lenovo laptop, Dell PC Desktop -4GB RAM, 100GB HD, DVD/CD-RW)
- Physical location/Employee Name
- Operating system release level
- Date placed in service
- Original cost

Any unused IT item/equipment should be stored in the IT storage room. This ensures that the item/equipment is safe place from theft or damage.

Physical inventory should be performed every year in order to validate the inventory and to determine maintenance issues needed for employee productivity. The inventory is conducted by the IT staff and the VP Finance reviews and signs the inventory report. An updated inventory list should be completed by September 30 of each year.

4.6.8 - Email - Procedure

Section: Operations
Subject: Email
Procedure: 4.6.8
Approved: December 15, 2015

Objective

This procedure provides appropriate guidelines for productively utilizing Carlton Trail College's email system that protects the employee and the College.

Procedure

Email Account Assignment

- Each employee will be assigned a unique email address that is to be used while conducting company business via email.

Ownership

- The email/electronic messaging systems are property of Carlton Trail College. All messages stored in company provided electronic messaging system(s) or composed, sent or received by any employee or non-employee are the property of the College. Electronic messages are NOT the property of any employee.
- The College reserves the right to intercept, monitor, review and/or disclose any and all messages composed, sent or received.
- The College reserves the right to alter, modify, re-route or block the delivery of messages as appropriate.
- The unique email addresses assigned to an employee are the property of the College. Employees may use these email addresses only while employed by the College.

Confidentiality

- Messages sent electronically can be intercepted inside or outside the College and as such there should never be an expectation of confidentiality. Do not disclose proprietary or confidential information through email.
- Electronic messages can never be unconditionally and unequivocally deleted. The remote possibility of discovery always exists. Use caution and judgment in determining whether a message should be delivered electronically versus in person.

- Electronic messages are legally discoverable and permissible as evidence in a court of law. Messages should not be composed that you would not want to read out loud in a court of law.
- Employees are prohibited from unauthorized transmission of the College confidential information, or privileged communications.

Security

The College employs anti-virus software. Employees are prohibited from disabling anti-virus software running on company provided computer equipment.

Although the company employs anti-virus software, some virus infected messages can enter the company's messaging systems. Viruses, "worms" and other malicious code can spread quickly if appropriate precautions are not taken. Follow the precautions discussed below:

- Be suspicious of messages sent by people not known by you.
- **Do not open attachments** unless they were anticipated by you. If you are not sure, **always verify** the sender is someone you know and that he or she actually sent you the email attachment. If you remain unsure, contact someone from IT.
- Disable features in electronic messaging programs that automatically preview messages before opening them.
- The College considers unsolicited commercial email (spam) a nuisance and a potential security threat. Do not attempt to remove yourself from future delivery of a message that you determine is spam. These "Remove Me" links are often used as a means to verify that you exist.
- Internet message boards are a fertile source from which mass junk e-mailers harvest email addresses and email domains. Do not use College provided email addresses when posting to message boards.

Inappropriate Use

- Email or electronic messaging systems may not be used for transmitting messages containing pornography, profanity, derogatory, defamatory, sexual, racist, harassing, or offensive material.
- The College prohibits discrimination based on national or ethnic origin, color, religion, age, sex, sexual orientation, marital status, family status, physical size or weight or disability Use of electronic messaging resources to discriminate for any or all of these reasons is prohibited.
- College provided electronic messaging resources may not be used for the promotion or publication of one's political or religious views, the operation of a business or for any undertaking for personal gain.

Termination of Employment

- Upon termination or separation from the College, the College will deny all access to electronic messaging resources, including the ability to download, forward, print or retrieve any messages stored in the electronic messaging system, regardless of sender or recipient.

Breach of Procedure

- Any employee in violation of this procedure is subject to disciplinary action, up to and including termination.

4.6.9 - Internet Usage - Procedure

Section: Operations
Subject: Software Usage
Procedure: 4.6.9
Approved: December 15, 2015

Objective

To provide appropriate guidelines for accessing and utilizing the Internet through the College network.

General

Internet services are authorized to employees in order to enhance their job responsibility. The Internet is an excellent tool but also creates security implications that the College must guard against. For that reason, employees are granted access only as a means of providing support in fulfilling their job responsibility.

Procedure

- User (which includes internet access and internet) accounts are approved for designated employees by the VP Administration and are set up by the Information Technologist to provide tools that assist in their work.
- Each individual is responsible for the account issued to him/her.
- Sharing user accounts or User-ID's is prohibited.
- Organizational use of Internet services must reflect the mission of the College and support its guiding principles.
- These services must support legitimate, mission related activities of the College and be consistent with prudent operational, security, and privacy considerations.

- The College has no control over the information or content accessed from the Internet and cannot be held responsible for the content.
- Any software or files downloaded via the Internet into the College network become the property of the College. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

Inappropriate Use

The following uses of College provided Internet access is not permitted:

- To access, upload, download, or distribute pornographic or sexually explicit material.
- Violate provincial or federal government law.
- Vandalize or damage the property of any other individual or organization.
- To invade or abuse the privacy of others.
- Violate copyright or use intellectual material without permission.
- To use the network for financial or commercial gain.
- To degrade or disrupt network performance.
- No employee may use College facilities or equipment knowingly to download or distribute pirated software or data.
- No employee may use the company's Internet facilities or equipment to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.

Breach of Procedure

- Any employee in violation of this procedure is subject to disciplinary action, up to and including termination.

4.6.10 - Mobile Phone - Procedure

Section: Operations
Subject: Mobile Phone
Procedure: 4.6.10
Approved: December 15, 2015
Revised: April 27, 2016

Objective

To provide guidelines on appropriate use of personally-owned mobile phones by employees at Carlton Trail College in order to maintain high productivity and safety at work.

General

Phone capabilities are integral parts of the College assets to help conduct business effectively. There are cases when field-staff use their personal mobile phones for business purposes. The guidelines herein should be read and understood by all employees using their personal mobile phones for school communications.

Procedure

Mobile Phone Allowance Eligibility

- The College may provide a monthly phone allowance to employees utilizing their personal mobile phones whose jobs require them to make calls while away from work or require them to be accessible for work-related matters. At the discretion of the VP Administration, the employee will be reimbursed through payroll for their personal mobile or smart phone service as follows:
    - $50.00 per month maximum allowance
- Any additional features are at the expense of the employee and upgrades or damages to the employee's phone are not reimbursable.
- Rates for reimbursement of personal mobile or smart phone services will be reviewed annually.
- Each recipient of a cell phone allowance must notify the College of his/her cell phone number and must continue to maintain the cell phone while in receipt of the allowance. It is the employee's responsibility to notify payroll of cancellation of their personal account.
- The cell phone contract will be between the carrier vendor and the employee. The employee will be solely responsible for all payments to the service provider. Only one cell phone allowance will be provided per employee.

Security

All cell phones used for College purposes should be password protected.

Use of Mobile Phone While Driving

All College staff driving on College business or driving a College-owned vehicle for any purpose, are prohibited from answering or initiating any electronic communication while the vehicle they are operating is in motion. This prohibition includes receiving or placing calls, text messaging, surfing the Internet, receiving or responding to email, checking for phone messages, or any other purpose related to employment or any other College or personally related activities not mentioned here while driving. This is to ensure safety of the employee, as well as the College property.

Any employee caught using his/her cell phone while driving by the authorities will have to pay the fine himself/herself and may be subject to disciplinary action.

Termination of Employment:

- In case of termination, layoff or dismissal of employment, the employee will have his/her College email account disabled in order to prevent him/her from getting business emails using the College domain (Please refer to Email Procedure regarding email accounts).
- In case when the employee receives monthly allowance from the College for the use of his/her personal phone for business purposes, application(s) on his/her mobile phone, which have been installed by the College will be deleted from his/her device. It is therefore, a must for an employee to make sure that his/her personal data are backed up and the mobile device be surrendered to the Information Technologist in order for the applications to be uninstalled.
- The phone allowance received by an employee will end upon the date of his/her separation from the College. The employee's supervisor needs to provide the VP Administration with the date of separation.

4.6.11 - Use of Personal Technology Device - Procedure

Section: Operations
Subject: Use of Personal Technology Device
Procedure: 4.6.11
Approved: December 15, 2015

Objective

To provide guidelines for the use of personally owned notebooks, smart phones, tablets and other types of mobile devices for work purposes. All staff who use or access Carlton Trail College's technology equipment and/or services are bound by the conditions of this procedure.

General

At Carlton Trail College, we acknowledge the importance of mobile technologies in improving business communication and productivity. In addition to the increased use of mobile devices, administrators, staff members, teachers and students have the option of connecting their own mobile devices to the College's network and equipment.

Procedures

Current Mobile Devices Approved for Business Use

The following personally owned mobile devices are approved to be used for work purposes:

- Mobile devices such as notebooks, smart phones, tablets, iPhone, iPad and removable media etc. using iOS or Android platforms.

Registration of personal mobile devices for business use:

- Employees when using personal devices for business use will register the device with the IT department, citing his/her relevant job title or department.
- The IT department will record the device and all applications used by the device

Personal mobile devices can only be used for the following business purposes:

- Email access using Outlook Microsoft Exchange to receive and send emails
- College telephone calls
- College internet access

Each employee who utilizes personal mobile devices agrees:

- Not to download or transfer College or personal sensitive information to the device. Sensitive information includes employee record systems, student personal information, such as Social Identification Number (SIN), account numbers, other personal identification numbers, credit card numbers and other types of structured information.
- Not to share unstructured information such as contracts, financial releases and College correspondence with students, companies and other stakeholders.
- Not to use the registered mobile device as the sole repository for Carlton Trail College's information. All business information stored on mobile devices should be backed up.
- To make every reasonable effort to ensure that Carlton Trail College's information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorized persons and all registered devices should be password protected.
- To maintain the device with current operating software, current security software etc.
- Not to share the device with other individuals to protect the business data access through the device.
- To abide by Carlton Trail College's Internet Procedure for appropriate use and access of internet sites etc.
- To notify Carlton Trail College immediately in the event of loss or theft of the registered device.

- Not to connect USB memory sticks from an untrusted or unknown source to Carlton Trail College's equipment.

All employees who have a registered personal mobile device for business use acknowledge that the College:

- Owns all intellectual property created on the device.
- Can access all data held on the device, including personal data.
- Will regularly back-up data held on the device.
- Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data.
- Has the right to deregister the device for business use at any time.

Keeping Mobile Devices Secure

The following must be observed when handling mobile computing devices (such as notebooks and iPads):

- Mobile computer devices must never be left unattended in a public place. Wherever possible they should be kept on the person or securely locked away.
- Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended.
- Mobile devices should be carried as hand luggage when travelling by aircraft.

Exemptions

- Any requests for exemptions from any of these directives, should be referred to the VP Administration.

Indemnity

- Carlton Trail College bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities.
- All staff indemnify Carlton Trail College against any and all damages, costs and expenses suffered by the College arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by the College.

Breach of Procedure

- Any breach of this procedure will be referred to the VP Administration who will review the breach and determine appropriate consequences, which can include confiscation of the device and or termination of employment.

4.6.12 - Password Construction Guidelines - Procedure

Section: Operations
Subject: Password Construction Guidelines
Procedure: 4.6.12
Approved: December 15, 2015

Objective

To provide best practices for the creation of secure passwords to reduce the chance of user accounts at Carlton Trail College from being compromised.

Procedures

Password Construction

Users should create passwords that meet or exceed the following guidelines:

- Contain at least 8 alphanumeric characters
- Contain both upper and lower case letters
- Contain at least one number

Passwords/passphrases should not:

- Be based on personal information, such as names of family, dates, addresses, phone numbers, etc.
- Be based on work information which can include but not limited to room numbers, building name, phone numbers, etc.
- User word or number patters like 1234321, abbaabba, abc123, etc.
- Be based on your username, nickname, screen name, etc.

For stronger passwords, the following characteristics can be followed:

- Contain at least 12 alphanumeric characters
- Contain both upper and lower case letters

- Contain at least one number (for example, 0-9)
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/)

You can make strong password/passphrases by simply substituting numbers for letters or words (or vice versa), such as: E equals 3, I equals 1, O equals 0 (zero), for equals 4, two equals 2, B equals 8, etc. Additionally, you should add a special character in the middle.

Protection

Password/passphrases are an important tool used by users to protect important resources. Some people are not accustomed to memorizing difficult passwords/passphrases that include numbers and/or special characters. Because of this many people choose to write down these passwords and keep them in unsecured locations such as posted on their computer screen, on post it notes around computer, under keyboard, etc. All users should follow the following security measure to protect their passwords and associated accounts:

- Passwords should be memorized and not written down or stored online. If one must write it down, it must be stored in a secure location.
- Passwords assigned to individuals should not be shared with anyone and should be treated as sensitive/confidential information.
- Anyone requesting an individual's password should be referred to the IT office and apply through specific channels with a just cause.
- User accounts with high level system privileges (such as administrators group in windows) should have a different password than other accounts held by that user.
- All default password/passphrases must be changed as soon as possible.

Maintenance

- It is important to remember that given enough time any password/passphrase can be guessed using currently available software. As such it is critical that passwords/passphrases be changed regularly. Users should not reuse any recent passwords/passphrases. Passwords are to be changed every 180 days.
- If an account is suspected of being compromised; change the password/passphrase if possible. If not, contact IT department to have it changed on your behalf.

Exceptions

- Any exception to this procedure must be approved by the IT department.

4.6.13 - Technology Equipment Disposal - Procedure

Section: Operations
Subject: Technology Equipment Disposal
Procedure: 4.6.13
Approved: December 15, 2015

Objective

To provide the guidelines for the disposal of technology equipment and components owned by Carlton Trail College.

Scope

This procedure covers any computer/technology equipment or peripheral devices that are no longer needed within Carlton Trail College including, but not limited to the following: personal computers, servers, hard drives, laptops, handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, compact discs and portable storage devices (i.e., USB drives).

General

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD/DVD-ROMs and other storage media contain various kinds of Carlton Trail College data, some of which is considered confidential. In order to protect sensitive information, all storage mediums must be properly erased before being disposed of. However, simply deleting or even reformatting data is not sufficient. When deleting files or reformatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

Procedure

Technology Equipment Disposal

- When Technology assets have reached the end of their useful life they should be sent to the IT department office for proper disposal.
- The designated IT staff will securely erase all storage mediums in accordance with current industry best practices.

- All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media, overwriting each and every disk sector of the machine with zero-filled blocks.
- No computer equipment should be disposed of via dumps, landfills, etc. Electronic recycling may be available in some locations around the Region. The designated IT staff will properly remove all data prior to final disposal.
- All electronic drives must be overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).
- Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, etc.
- The IT staff will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.
- Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

Management of Disposed Equipment

- Any equipment not in working order or that the College no longer needs may be donated or disposed of according to current environmental guidelines. With the authorization of the VP Finance, the IT department may contact external organizations or send notification to staff to donate or properly dispose of outdated technology assets.
- Prior to leaving Carlton Trail College premises, all equipment must be removed from the Information Technology inventory system.

Procedure Compliance

- The Executive team will verify compliance to this procedure through various methods, including but not limited to, College reports, internal and external audits, and feedback to the IT staff.

Exceptions

- Any exception to the procedure must be approved by the VP Finance in advance.

Breach of Procedure

- An employee found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment.

4.6.14 - IT Disaster Recovery Plan - Procedure

Section: Operations
Subject: IT Disaster Recovery Plan
Procedure: 4.6.14
Approved: December 15, 2015

Objective

To define the requirement for a baseline disaster recovery plan to be developed and implemented by Carlton Trail College that will describe the process to recover IT systems, applications and data from any type of disaster that causes a major outage.

Scope

This procedure is directed to the IT staff who are accountable to ensure the plan is developed, tested and kept up-to-date. This procedure is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

General

It is important to realize that having a contingency plan in the event of a disaster gives Carlton Trail College a competitive advantage. This procedure requires IT staff to diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered. The Disaster Recovery Plan is often part of the Enterprise Risk Management Plan.

Procedure

Contingency Plans

The following contingency plans must be created:

- Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
- Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
- Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.

- Criticality of Service List: List all the services provided and their order of importance.
- It also explains the order of recovery in both short-term and long-term timeframes.
- Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.
- Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where the equipment may be obtained.

After creating the plans, it is important to practice them to the extent possible. IT staff should set aside time to test implementation of the disaster recovery plan. Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, should be reviewed an updated on an annual basis.

Procedure Compliance Measurement

- The Executive Team of Carlton Trail College will verify compliance to this procedure through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to IT staff.

Exceptions

- Any exception to the procedure must be approved by the Executive Team in advance.

Breach of Procedure

- An employee found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment.