4.18 – IT Security Management - Policy

Approved: March 30, 2021

1. Purpose:

Carlton Trail College is committed to the Information Technology security management, including the protection, confidentiality, integrity, availability, reliability and recoverability of the College's IT systems and data on our network.

2. Scope:

Everyone at the College has a responsibility for the proper handling and protection of confidential information as set out in this policy. These policies apply to the entire College community including faculty, staff, and students. The Policy is supported by procedures that describe what must be done to be in compliance.

3. Definitions:

IT systems and data - all IT hardware, computer software, electronic data, and associated peripherals.

4. Policy:

a) The College will reduce the risk of negligent or deliberate system misuse and protect the confidentiality, authenticity, integrity and continuity of Information Technology systems and data.

b) The College will ensure an information security management framework is in place and remains current. The College's Senior Leadership Team will approve the framework every three years.

c) The College will restrict access to digital information on the College network, as well as access to networks and network services, on the basis of business security requirements, and access control rules will take account of policies for information dissemination and authorization.

d) The College will restrict the physical access and security to the College's data-processing facilities and equipment.

e) The College will ensure measures are in place to prevent disruptions to information systems and loss of digital data and ensure business continuity.

f) The College will ensure compliance with applicable legislation and contractual requirements, including but not limited to intellectual property rights for software or document copyright, design rights, trademarks, patents and source code license.

g) Staff are required to comply with information security policies, procedures, and practices established by the College. If multiple policy statements or security standards are relevant for a specific situation, the most restrictive security standards will apply.

Failure to comply with established policies and practices may result in loss of computing privileges and/or disciplinary action.

h) Students are required to comply with information security policies, procedures, and practices established by the College. If multiple policy statements or security standards are relevant for a specific situation, the most restrictive security standards will apply.

Failure to comply with established policies and practices may result in loss of computing privileges and/or disciplinary action as per student policy.

5. **Responsibility:**

VP Administration	Has the overall responsibility for the implementation of the IT policies and procedures.
Systems Administrator	Will develop, implement, monitor and communicate procedures to ensure appropriate IT controls.
Board of Directors	Will have final approval over policy.

4.18 – IT Security Management - Procedure

Approved: March 30, 2021

General Information

Regional offices and program locations IT infrastructure exist within Community Net, a government-controlled and secured infrastructure that provides additional layers of protection from the public internet.

At all levels within the organization, anti-virus and anti-malware software will be installed with automatic scanning and updating features enabled to help prevent unauthorized intrusions. In the event an infection occurs, staff and students are to contact the IT staff members immediately so it can be quarantined and removed. After any the occurrence of any IT incident, the IT staff will use the information gathered, identify current gaps, and implement mitigation strategies to prevent future occurrences. Information regarding threats will then be communicated to the staff and students.

1. Security

Server level securities are restricted to the IT staff, the VP Administration, the VP Finance and approved third party vendors. However, all work and access to the college network by third party vendors is granted by Information Technology staff upon approval of the VP Administration.

Security of College data on College-issued mobile devices shall follow the College IT policy concerning information security and mobile device management.

2. Information Security Management Framework

Management of Information Security will be maintained to initiate and control the implementation of IT security measures within the organization in accordance with business requirements and relevant laws and regulations. The VP Administration will maintain the IT security management framework, assign security roles and co-ordinate and review the implementation of information security across the College.

The College's Systems Administrator will be responsible and accountable for ensuring that the appropriate information security controls are implemented within the organization's information systems.

The management, development, review, and evaluation of IT security framework will be reviewed by the Systems Administrator and VP Administration annually unless significant changes have occurred that would impact current policies. The criteria used during this evaluation includes current business requirements, risk assessments, relevant laws and regulations, and data risk assignment with high and low risk areas being clearly identified. Examples that would initiate the review process outside of the regular timeline include changes to the organizational environment, business circumstances, legal conditions, or technical environment within the College. This will ensure their continuing suitability, adequacy, and effectiveness of the information and the security measures in place.

As part of the security within the College, local authorities (i.e. Law enforcement, Fire Department, etc.) as well as any external third parties (i.e. Support services, vendors, etc.) will be contacted to take action when required as outlined in the IT Disaster Recovery Plan and the College Emergency Preparedness Plan. These contacts and their associated information must be continually maintained to ensure business continuity and is a large part of the contingency planning process and are to be reviewed on an ongoing basis. The System Administrator shall be responsible for maintaining this list.

The IT Department as well as the Senior Leadership and Management staff within the College will be responsible for reviewing regulatory and legislative compliance with information processing and procedures within their area of responsibility. They will also review and properly classify the sensitivity of their information and ensure proper access is in place. Information Technology is responsible for recording and executing any information security requests through their help desk ticket system to allow for proper tracking, management, and a historical record of the request.

3. User Access Controls and Authorization

The College has controls to secure the access to information (both cloud-based and on-premises, information processing facilities, and business processes. Access controls are the basis of business and security requirements and take into account the policies for information dissemination and authorization.

The College follows a minimalistic approach to information access. Managers of each Department will be responsible for requesting access control changes when required to ensure that access to information is appropriate for their area to be approved by the VP Administration. Information Technology will maintain a listing of information owners and access groups through the network (Active Directory).

User account access request must be submitted by supervisors to IT via their Help Desk ticketing system. This includes, but is not limited to, any access to network resources, data shares, email, security access groups, physical hardware within any College location, or any other form of secure access to computer data information within the College. Users are required to follow the College's policies and procedures in the use and access of information whether physical or digital.

4. Account Authorization and Creation

Prior to computer network access being granted to a user (staff or student), a signed "Statement of Understanding" form must be submitted to Human Resources.

Temporary passwords are initially issued, and the user will be prompted to change the password immediately after the first successful login. Passwords that are created MUST follow procedure 4.6.1.2, *Password Construction Guidelines.*

The authorization procedure for determining who is allowed to access which network and networked services is established by the College’s organizational chart and authority matrix and tracked via the Help Desk ticket system.

Active Directory allows for the management of the computer network domain security measures for individual users and user groups. These accounts are also connected to the network drive scripts that will map connections to specific shares related to the security group (i.e. Programs, Accounting, Instructors, Students, etc.). These security groups are further subdivided into access permissions for easier management (full control, read only, manage, etc.). These security groups assign multiple levels of permissions to various areas within the network and are managed by the IT Department. When permissions are assigned, they are to be the minimum required permission level for the user to meet the requirements outlined from their supervisor's request via the Help Desk.

Each user receives a username and password, and all computer hardware is configured to include local security settings to restrict unauthorized installation of software and hardware without an administrator level password. These devices have pre-installed virus and malware software, and, if they are on the domain, they will also have mandatory screen lock timers installed.

5. Network Access

Network access required by staff is requested by management staff to IT using the Help Desk. The IT staff members will then review the request ensuring that the access requested aligns with minimum access requirements. The IT Department will communicate directly with the requestor any concerns with the request.

Controls are present to protect access to network connections and network services as well as the means used to access networks and network services (i.e. access to an internet service provider or remote access). These access controls are implemented through the use of network user permissions and group permissions created through the College's Microsoft Active Directory service.

These permissions can only be modified by the IT staff members. Remote access to network resources is available for email services via Office 365 using an internet browser, for network file access. This method requires an active college user account and password to access, and the individual can only access areas in which they have permission to do so.

6. Removal of Access Permissions

User accounts are only active while the individual is a member of the staff or student body within the College. For staff who no longer require access, or their access requirements change (due to changes in roles, positions, etc.) the manager will notify the IT staff (via Help Desk) and Human Resources immediately to either remove network access by deactivating the account or adjusting permissions as required. For students, the Coordinator of the program they are enrolled in will notify IT. Once the changes have been completed, the requestors will be notified. The IT staff will disable accounts as soon as possible in the same day as the submitted request to ensure optimal security is kept in place. In the event of a staff departure, the IT staff members will work with the staff member's manager to review their email mailbox and local/network data with the intention to retain anything deemed essential and to remove the remaining information from the system. This process will occur within one week of the effective termination date, unless otherwise requested by the supervisor.

Student accounts are to be disabled and removed after the completion date of the program unless otherwise requested by the student's coordinator due to withdrawals or extensions.

7. Virus and Malware Log Review

The College has installed Cylance and Cylance Optics on all endpoints at the College to track and monitor any suspicious activity. The security logs, which are available through Cylance Optics, are reviewed regularly by the Systems Administrator to ensure that infections are not present, and the proper function of the management system is in place. This should take place at a minimum of once a week, unless otherwise notified by the system, staff, or students.

Additional security measures may be added as hardware and software changes occur.

8. Physical Location Access and Security and Asset Management

a) Physical Location Access and Security

Critical and sensitive processing facilities (i.e. server rooms, wiring closets, network racks, etc.) are housed in secure areas and protected by security barriers and entry controls. These areas must be physically protected from unauthorized access, damage, and interference.

Restrictive access is in place for these areas with the only key holders being the VP Administration, VP Finance, President & CEO, the IT staff members, and the Facilities Technician. Non-IT staff may only access these areas under direct permission and supervision of IT or the VP Administration. Third party vendors who need access to these areas must have identification badging visible and are only granted access where required. Access will be revoked upon completion of work in these areas. Under no circumstances will public access be granted to these areas.

These areas must reflect the minimum indication of their purpose and have no obvious signage outside or inside the building to identify the presence of information processing activities. Staff members are to only be aware of the existence of, or activities within, secure areas on a need-to- know basis. Any unsupervised work in a secure area will be avoided for safety and prevention of malicious activities.

Photographic, video, audio, or other recording equipment, such as mobile device cameras, will not be allowed unless authorized by the Systems Administrator.

The College will give consideration to any security threats presented by neighbouring premises, fire, water, below ground level facilities and explosions. Consideration will be given to avoid damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man- made disasters.

b) Asset Management

IT staff will perform spot checks around the campus locations to detect any unauthorized removal of property should it not be reported by staff members. These checks should be carried out following relevant legislation and regulations. Any equipment that is being utilized off campus would be checked by the staff members present and responsible for the location. Should college staff find any issues they are to report them to IT or their supervisors immediately upon discovery. Hardware is to be physically secured in locked cabinets if the room or location is not restricted to College staff only. In these instances, staff members are responsible for the removal of the hardware at the end of each class day or session and are to keep the equipment secure.

As per the I.T. Asset Management Procedure, when disposing hardware, all sensitive data must be removed either through physical destruction, high-level software deletion and overwriting techniques, or any method to make the original data irretrievable beyond a standard delete or format function. If some data is deemed critical and high risk, the storage medium is to be physically destroyed in a fashion to ensure it is non-recoverable.

All hardware and software purchases are to be managed by Information Technology. Delivery of any and all physical computer hardware will take place in areas separate from any secure IT areas within the campus locations. (I.E. server rooms, network cabling locations, etc.) These areas must remain secure at all times.

Equipment will be catalogued into the *WASP Asset Cloud* Inventory System by the IT staff, or designated personnel, when received along with information about the hardware and its intended location. These records are maintained to allow for proper equipment tracking and inventory as per the IT Asset Management policy. This hardware will not to be taken off-site without prior authorization, and the individuals permitted to do so must be clearly identified. Staff must also record when the item has been returned and report any issues to the IT staff if present.

Off-site hardware will exist in a secure and off-keyed location to prevent any unauthorized access (i.e. rural program locations, or locations inside another building from a different business). The responsibility for security of these locations falls on the staff member(s) at the site. They will ensure all hardware and data is secure along with the physical access to the location. Should a rural site location not provide secure access, the college staff member will be responsible to physically remove the equipment and data when leaving the premises.

c) Off Campus Locations and Teleworking

Off campus work at rural sites or through teleworking will have appropriate security arrangements and controls in place at the site in accordance with the College's policies and procedures. Suitable protection measures of the site must be in place to prevent against theft of equipment and information, unauthorized disclosure of information, unauthorized remote access to the organization's internal systems, unauthorized use by non-College employees and students, or misuse of the equipment and/or facilities.

These measures will be enforced in conjunction with the user's supervisor and IT. The Facilities Technician may be consulted in certain situations if required. Ongoing reviews of these sites shall continue during use by supervisory staff to ensure that the security measures in these areas remain consistent.

In a teleworking situation, the employee is responsible for protecting College data by adhering to the College's Information Technology Use and Management procedure. When teleworking, employees must comply with all College guidelines to protect College data and the use of computer hardware and software, including, but not limited to:

- Using strong passwords
- Store sensitive documents on Office 365 or local area network storage, not local devices.
- Devices being used to perform College work must be up to date with patches and have current anti-malware software installed and configured.
- College work should be performed on devices running current versions of software.

9. Business Continuity and Prevention of Digital Data Loss

Operating procedures are documented where required as well as defining the segregation of duties and responsibilities to reduce the risk of negligent or deliberate system misuse. This includes areas from desktop preparation checklists, installation guides, disaster recovery plans, etc. This documentation is updated as required pending system upgrades or changes, or infrastructure changes.

10. Capacity Management

Capacity management will occur through ongoing reviews of network and user activity, capacity requirements, system tuning and resource allocations, and overall monitoring to ensure the availability and efficiency of all related systems. Projections of future capacity requirements will take into account new business and system requirements as well as current and projected trends in the organization's information processing capabilities. In doing so, the College will maintain a level of separation between the operational (production) and test environments as necessary to prevent any operational issues being identified. This will allow for the appropriate control measures to be implemented minimizing impacts on daily operations.

11. Virus and Malware Prevention

Virus and malware prevention software is in place to prevent possible infections/intrusions at both the user and server level. Instances of infections are reported locally as well as to the management server for review and removal by the Information Technology staff.

User and server level hardware protection is protected and centrally managed by the same software platform (currently Cylance and Cylance Optics). This platform has the capability for automated scanning and consistent update installation schedules. This also ensures timely patching occurs and any intrusion or infections are quarantined, reported to the IT staff members, and then removed. In the event a quarantined item cannot be automatically removed, IT will be required to remove the threat.

If an infection occurs, the equipment in question is immediately quarantined and physically removed from the network to prevent further contamination. Data is backed up to a separate external storage device at Horizon Computers and the equipment is scanned to remove the infection compromising the system. The IT staff members are notified of infections, and it is also the responsibility of the user to report these issues immediately so they can be dealt with. If the issue cannot be resolved or repaired properly, the hardware (computer, laptop, server, etc.) will be completely erased.

After which the item will be restored from backup (in the case of server issues), or reimaged (in the case of user level hardware issues) with the data being scanned for potential threats prior to being placed back onto the device. After such an occurrence, a review of the cause shall take place by IT and reported to the VP Administration. The review shall include possible reasons for infection, as well as prevention options to stop any reoccurrence. Regular information regarding this shall also be sent out to staff to help inform them of risks and the process of reporting them.

12. System Software Update Management

Microsoft Windows Desktop and Microsoft Server platform updates will be automated and set to search and install updates daily, if available. A Microsoft Windows Services Update Server (WSUS) is used for both desktop-level and server updates at the campuses, finding the released updates and deploying them out to all connected computers. External bandwidth use is reduced by using this method.

Automating the process ensures the platforms are up to date and will help to promote functionality, security, and performance issues from occurring. In some cases where automation is not available, computers will be manually updated by the IT staff.

13. Data Backup and Recovery

Server data is stored directly on the servers in Humboldt. These devices contain all the network data from the respective campuses and office locations. All server and network data is backed up to these devices to an offsite device at Horizon Computers. This occurs using the separate SaskTel internet connection. The purpose of this process is to allow for file, server, and site recovery as outlined in the disaster recovery plan.

All relevant Office 365 data is backed up through a SaaS (Service as a Software) called NetApp. This includes Microsoft Exchange, SharePoint online, and OneDrive for staff members. This data is stored within Canada through Amazon S3 storage.

All server backups are automated and occur each evening, notifications of successful backup completions are emailed to the IT staff. If any failures or issues occur, they are automatically notified by email.

Backups are tested regularly with file recoveries being tested monthly and larger scale server recoveries tested annually. Backup data and logs are verified weekly by the Systems Administrator to ensure proper function and to address any issues. Server logs are periodically reviewed to ensure proper function of the hardware.

The data centre components are configured with fault tolerance capabilities to ensure business operations are not impacted by a single failure of component. Should a situation occur where the fault tolerance has failed, IT will immediately notify the VP Administration and determine a solution for the issue.

All IT-related maintenance activities are executed in a manner that will minimize disruption to business operations, with routine maintenance occurring outside of business hours. Once the root cause of any failure has been determined, steps are taken to ensure the issue will not be able to occur in the future. The information is summarized and reported to the VP Administration and documented by email for historical reference.

Information security continuity is addressed through the College business planning. All college staff are responsible for protecting information within reasonable expectations according to the event (i.e. natural disasters, accidents, equipment failure, and deliberate actions).

14. Change Management

The management of changes within IT is critical to ensure the integrity, consistency, and availability of technology services.

All changes to the Carlton Trail College production environment will be tracked via a Help Desk ticketing system. Service requests will be entered into and managed via the Help Desk by users to ensure changes are centrally tracked, approved, reported, and enforced in a reliable and consistent manner. Requests must be reviewed and approved by the Systems Administrator prior to execution to ensure a proposed change does not compromise the stability of the production environment.

Changes to the production environment are:

a. Documented using the Help Desk System.
b. Implemented using the appropriate process and authorization
c. Approved by the Systems Administrator
d. Communicated effectively that all responsible parties are aware of the change assignment and all user communities are aware of any potential impact.

The Systems Administrator (or Educational Technologist in collaboration with the VP Administration in their absence) is notified of the potentially necessary change and will be responsible for obtaining the facts, justification, and full description of the requested change. This includes reviewing all change request notifications submitted by staff members or systems owners, obtaining all communication and documentation necessary, resolving any scheduling conflicts that may arise, providing feedback concerning priority, risk, and impact of change, and, where applicable, communicating to the user community affected by the change prior to and after the implementation. It is the responsibility of IT to determine overall priority and assess the risk of the requested change, as well as communicating with the supervisory and management staff required to gather the required information as part of the approval and implementation process.

To ensure the information security implications of all change requests are reviewed, the assessments made during the process will include the consideration of implications to the security of personal information (Social Insurance Number, date of birth, etc.), the security of sensitive or confidential data, the security of College equipment, and compliance implications. In cases where potential high security threats are determined, these findings and concerns can be presented to the VP Administration for further approval at a management level.

The Information Technology department is responsible for evaluating, testing, installing, maintaining, and documenting all software and operating systems that are installed in the College including staff computers, computer labs, classroom computers and mobile lab computer carts.

All staff must follow the software purchase and installation procedure as outlined in Procedures 4.6.3 and 4.6.4. All software requests must be done through the Help Desk ticketing system.

15. Legislative and Contractual Compliance

The Senior Leadership Team and Managers are responsible for regularly reviewing regulatory and legislation compliance with information processing and procedures within their area of responsibility. Supervisors are responsible for classifying the sensitivity of their information and ensuring that the proper auditing of information access is in place. IT will be responsible for recording and executing any information security requests. As part of the verification of private and personal information, Information Technology must be able to provide security reports to management on an as needed basis.

16. User Compliance with IT Policies and Procedures

Once a computer user account has been created and granted access to the college network, either staff or student, there is an expectation that proper usage guidelines will be followed during this time. Users are expected to agree and adhere to these guidelines while operating within the college network, as well as ensure that their overall security is consciously maintained and not allow their information or access to be compromised. The overall responsibility of the account and its access belongs to the user and as such, the user will be held accountable for any actions taken while using their account. The agreement, as well as the areas outlined is contained within the “Information Technology Policies (4.6)" in which all users both staff and student are required to review and sign prior to being granted an account.