Information Technology Policies and Procedures

7.0 **INFORMATION & MATERIAL MANAGEMENT**
7.01 IT Security Management
7.02 Anti-Spam
7.03 Cell Phone
7.04 Records Retention and Disposal
7.05 Backup

POLICY 7.01

Subject: **IT Security Management**

Approval/Amendment Date(s): May 3, 2015

Associated Procedure/Documents: Procedure G 7.01 IT Security Management, Policy 3.03 Computer Use Policy & Procedural Guidelines Acceptable Use Agreement

Next Review Date:

Purpose:

North West 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.

1.0 Scope:

Everyone at the College has a responsibility for the proper handling and protection of confidential information as set out in the Policy Statements. 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.

2.0 Definitions:

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

3.0 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 Executive Management 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.

4.0 Responsibility:

Executive Sponsor	Has the overall responsibility for the implementation of the IT Management policies and procedures.
Coordinator, Information and Technology	Will develop, implement, monitor and communicate procedures to ensure appropriate IT controls.
Executive Management	Will have final approval over policy.

* * *

POLICY 7.02

Subject: **Anti-Spam**

Approval/Amendment Dates(s): June 10, 2016

Associated Procedure/Documents:

Next Review Date:

Purpose:

North West College is committed to ensuring compliance with the provisions of Canada's Anti-Spam Legislation and associated regulations (CASL). The purpose of this Canada's Anti-Spam Legislation Policy is to define the roles and responsibilities of North West College and its employees.

1.0 Scope:

This policy applies to all employees of the College (full-time, part-time, contract and casual), and/or any other persons who have been given access to a College email account.

This Policy applies to all employees of the College when sending electronic messages from any College account or owned domain name for the purpose of promoting, advertising, marketing, or selling a North West College product or service or promoting the North West College brand.

2.0 Definitions:

Altering transmission data – Manipulating the information regarding where, how or when the communications is sent, so the electronic message is delivered to a destination or recipient that is different or in addition to and unbeknownst to and without the original sender's express consent.

Commercial activity – Anything of commercial nature promoting a product, goods or service to a person or inspires a person to engage in the purchase of that product, good, or service.

Commercial Electronic Messages (CEMs) – is any electronic message that is sent for the purpose of marketing or advertising.

Express consent – Permission which has been given in writing by an individual to receive messages.

Implied consent – Consent that the individual is knowingly giving permission can be confirmed based on the nature of the services being provided.

Social media – Digital technologies and practices enabling people to use, create, and share content in many forms such as text, images, audio, video, and other multimedia communications. Examples include blogs, social networking websites and video sharing websites.

3.0 Policy:

a) All employees are governed by this Policy when sending CEM's and are responsible for ensuring they adhere to CASL requirements for the sending of CEMs and unsubscribing an electronic address from receiving future CEMs.
   All outbound CEMs will:
   i) identify the College sender (department or employee) of the message;
   ii) include the College senders (department or employee) contact information; and provide an unsubscribe mechanism.

b) Social media direct messages may only be sent if it is in response to an inquiry. Only College employees who have been authorized to act on behalf of the College may use external social media channels to communicate for the College's business purposes.

c) All employees will ensure they have prior implied or express consent to send a CEM to an electronic address.

d) All CEMs sent by employees (including when using third parties to send CEMs on behalf of the College) will be sent in accordance with the requirements outlined in the CASL.

a) If implied consent does not exist, it is necessary to obtain express consent. Express consent must include:
   i) The purpose for which the consent is being sought;
   ii) iThe College department/employee requesting the consent;
   iii) The contact information of the College department/employee sending the CEM; and
   iv) A statement that consent can be withdrawn at any time.

f) Verbal consent (i.e. orally obtained consent) and written proofs of consent must be stored by each department/employee for a minimum of three (3) years.

g) Employees must verify the unsubscribe status of electronic addresses before sending any CEMs.

h) Electronic mail lists must be updated within ten (10) business days of receipt of unsubscribe requests.
i) The Department Supervisor of each individual department/employee is responsible for ensuring that employees in respective departments receive CASL awareness training.
j) The department/employee supervisor of each individual is responsible for ensuring that their respective department/employee is complying with CASL.

4.0 Responsibility:

The Director of Finance and Administration is responsible for all aspects of this policy.

* * *

POLICY 7.03

Subject: **Cell Phone**

Approval/Amendment Date(s): August 16, 2016

Associated Procedure/Documents: Procedure G 7.03 Cell Phone, Policy 7.02 Anti-spam policy, Policy 2.01 Employee Code of Conduct

Next Review Date:

Purpose:

North West College (NWC) recognizes the importance of cell phones in undertaking our business and is committed to establish guidelines regarding the purchase and usage of such devices and define the roles and responsibilities of North West College and its employees.

1.0 Scope:

This policy applies to all employees of NWC (full-time, part-time, contract and casual), and/or any other persons who have been granted a NWC email account).

This Policy applies to all employees of NWC who have been assigned and/or operate a College cell phone.

2.0 Policy:

a) Request for a College cell phone must be made to the President or Director responsible. Eligibility and approval of a College cell phone is determined by the President and/or the Director responsible. The cell phone device must be essential for the employee to properly perform his or her required duties. The following criteria must be used when approving requests for communication devices.
   i) The employee's job duties are critical to the operation of the College and immediate response may be required.
   ii) The employee needs to be accessible after normal working hours.
   iii) The employee must be accessible in the event of an emergency.
   iv) The employee is frequently away from access to traditional land based phone services.

v) The employee's job requires them to be mobile with direct office contact and access to email is essential to their responsibilities.

b) The assignment of a College-owned phone is made to allow employees to conduct College business. There may be circumstances when an employee with a College-owned communication device uses it for personal reasons. To the extent that such personal use results in increased charges to the College, the employee may be responsible for reimbursing the College for the cost of excess charges.

c) Use of College owned communications devices shall be in accordance with other relevant College policies (i.e.: NWC Anti-Spam policy and Employee Code of Conduct).

d) It is the responsibility of the end user:
   i) to ensure all cell phones are password protected at all times and employees shall not allow non-College employees use of these devices;
   ii) employees are expected to use the devices in a manner that is lawful, moral and respectful at all times;
   iii) employees are expected to protect the devices from loss, damage or theft; and
   iv) employees must turn off roaming when using phones out of the country.

e) All cell phones issued by NWC, are the property of the College. Employees should have no expectation of privacy. Phones may be recalled at any time and remote wiping of all data will be performed if deemed necessary.

f) Employees on a leave of absence may be required to return their device during the leave.

g) Upon resignation or termination with the College, phone numbers will be cancelled or transferred to a new College employee.

h) The Director is responsible for management of all devices authorized to staff members under their responsibility and therefore must notify the Director of Finance and Administration and the Coordinator of Information Technology when changes, cancellations or transfers of a device need to be made.

i) It is the responsibility of the Information Technology department to maintain a process for requests and support of cell phone devices and to ensure remote memory wiping on capable devices upon departure from NWC.

j) The Director of Finance and Administration is responsible to maintain a list of all College authorized cell phones and request forms, as well as monitor billings.

3.0 Responsibility:

The Director of Finance and Administration is responsible for all aspects of this policy.

* * *

POLICY 7.04

Subject: **Records Retention and Disposal**

Approval/Amendment Date(s): December 5, 2019

Associated Procedure/Documents: Procedure G 7.04 Records Retention and Disposal

Next Review Date:

Purpose/Philosophy:

North West College has a lawful duty to keep and maintain records and books of account pursuant to the Income Tax Act, Employment Insurance Act, Canada Pension Plan, as well other other federal and provincial regulatory bodies.

1.0 Policy:

All staff must adhere to the appended procedures for record retention/destruction and abide by the related periods of time for which records must be retained before they can be destroyed.

* * *

POLICY 7.05

Subject: **Backup**

Approval/Amendment Date(s): January 6, 2022

Associated Procedure/Documents: Procedure G 7.05 Backup

Next Review Date:

Purpose:

This document sets out North West College's policy towards taking backups of its information assets, including their frequency, storage, retention, documentation and restoration.

1.0 Scope:

This policy applies to all employees of NWC (full-time, part-time, contract and casual), and/or any other persons who have been granted a NWC email account).

2.0 Policy:

Backup is the process by which you make a copy of your work for safekeeping in an alternate location, in case your current work becomes lost or corrupt. The backup copy is only as recent as the last time it was modified. The higher the value of the files or the more work you do, the more frequently you should back up your work.

The backups of essential business information and software should be taken according to a comprehensive schedule. Adequate back-up facilities should be provided to ensure that all essential business information and software could be recovered following a disaster or media failure.

Back-up arrangements for individual systems and related data should be tested according to a formal schedule to ensure that they meet the requirements of business continuity plans.

Definitions of data

Confidentiality: Ensuring that information is accessible only to those authorized to have access.

Availability: Ensuring that authorized users have access to information and associated assets when required.

Critical: Degree to which an organization depends on the continued availability of the system or services to conduct its normal operations.

Integrity: Safeguarding the accuracy and completeness of information and processing methods.

Backup

- All applications, operating systems, data (including databases), user configuration information and hardware configuration information (where applicable) must be backed up at least weekly.
- Separate systems specific backup procedures must be developed in accordance with server, files, folders and data. These procedures must be documented and implemented during (and as part of) system implementation.
- The Backup Procedure will determine the type of backups to be performed, the periodicity or schedule of the backup, the protection to be provided to backup media based on the criticality of the information backed up
- This may be achieved using a combination of image copies, incremental backups, differential backups, transaction logs, or other techniques.
- Backed up data that is confidential must be stored in encrypted form if off site.
- Restoration of backups will require specific and appropriate authorization and must be performed in accordance with the Restoration Procedure.
- Systems Administrators shall perform a verification process on the back-up data to make sure that it is backed up successfully.
- Systems Administrators shall perform a backup before and after installing batches or upgrades or making any configuration changes on the system.
- A copy of backups shall exist at the opposite campus in case of complete lost at a campus.
- An Airgapped (backup on an external hardrive not left connected to the system) Shall be taken twice annually and stored in a safe place ie the safe at each location.

Testing of Backup Media

Systems Administrators must check the backup media (drive Space) regularly and make sure that there is adequate space for the backups and test the integrity of the backups monthly.

After completion of backup testing, all data must be safely erased from the test environment.

Testing of Restoration Procedures

The IT Department is to be responsible for testing system software and data backups by restoring a sample of the backups according to a formal schedule in the test environment. The Information Technology Coordinator is to be responsible for controlling and supervising backup testing.

Restoration procedures must be regularly checked (at least on a bi-annual basis) and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

Backup Frequency

Availability and Integrity of Data

The frequency of data backup for each system must be determined by considering the 'Availability' and 'Integrity' required for the server/data

Backup Cycles/Generations

At least **5** years of back-up information must be retained for important business applications and critical data of Accounting and Student Information Database.

Daily and weekly backup (on-site storage) to be readily available for the recovery of lost **or damaged** files.

Backup Storage

Off-site Storage

Backups must be stored at apposing campuses at a periodicity in order to be available in the event of a disaster, or for long term storage.

A minimum level of back-up information, together with accurate and complete records of the back-up copies and documented restoration procedures, must be stored in a remote location, at a sufficient distance from College to escape any

damage from a disaster at the main site.

Physical and Environmental Controls

Back-up information must be stored off site and given an appropriate level of physical protection (locked and secure). They must also have environmental protection (dry and low humidity).

An air gapped backup (external hard drive removable from the system) must be taken monthly and securely stored at site. An air gapped back up must be taken quarterly and securely stored off site.

3.0 Responsibility:

Of this policy is the Information Technology Coordinator and the Director of Finance and Administration. The Information Technology department is responsible for maintenance and accuracy of the policy.

* * *

PROCEDURE G 7.01

Subject: **IT (Information Technology) Security Management**

Approval/Amendment Date(s): May 3, 2015

Associated Procedure/Documents: Policy 7.01 IT Security Management

Next Review Date:

G.7.01.01 Risk Reduction and Data Protection

All staff and are required to read and sign an agreement to the Computer Use Policy and Procedural Guidelines Acceptable Use Agreement (per Policy 3.03), which explains their expected use of the computer systems and responsibilities of the user within the College. This agreement also outlines areas and definitions of misuse and consequences referenced in the College disciplinary policies.

Upon receipt of a signed computer use agreement, user permissions are assigned at a minimally required access level as requested by their direct supervisor, or as pre-determined due to their roles and responsibilities (i.e. Student access: minimal network access to specific drives). These permissions will allow specific access to network resources based on their assigned security group(s) within the college's Active Directory service. Local permissions are also minimized, and changes to the hardware and software at the desktop level are not allowed. Any changes are to be made by the IT Department only. These include software installations and hardware changes.

To prevent unauthorized local computer access, all users are required to secure their computer hardware when leaving it unattended using screen locks and passwords. Local computer hardware (desktops/laptops) will be preconfigured to automatically lock the screen after 10 minutes of inactivity, and require the user to sign in again to gain access.

To prevent external vulnerabilities and access from occurring, both sites will have physical firewall hardware to block unauthorized accesses as well as provided internal content filtering and protection against potentially malicious websites and internet traffic. These devices are automatically updated, and are monitored by the IT Department. The Battlefords and Meadow Lake campuses also exist within Community Net, a government-controlled and -secured infrastructure that provides additional layers of protection from the public internet.

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

At all levels within the organization antivirus and antimalware 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 this the IT will use the information gathered to prevent future occurrences. Information regarding threats will then be communicated to the staff and students.

Security of College data on College-issued mobile devices shall follow the College policy around information security.

G.7.01.02 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 Director of Finance and Administration will maintain the IT security management framework, assign security roles and co-ordinate and review the implementation of information security across the College.

Once a set of policies is defined they are to be submitted to the Policy Committee for review and to participate in the policy review and approval cycle. Once approved, the policies are published and communicated to employees and any relevant external parties that may be impacted by the change. This process would also occur with the review cycle timelines established by the Policy Committee.

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.

The College's IT Coordinator 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 IT Coordinator and Director of Finance and Administration annually unless significant changes have occurred that would impact current policies. Examples that would initiate the review process 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 (DRP) and the College Emergency Response Plan (ERP). 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 IT Department as well as the supervisory 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 service desk ticket system to allow for proper tracking, management, and a historical record of the request.

G.7.01.03 User Access Controls and Authorization

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

The College follows a minimalistic approach to information access. Supervisors of each business unit will be responsible for requesting access control changes when required to ensure that access to information is appropriate for their area. 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 Service 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.

G.7.01.04 Account Authorization and Creation

Prior to computer network access being granted to a user (staff or student), a signed "Computer Use Policy and Procedural Guidelines Acceptable Use Agreement" form must be submitted to Information Technology staff after being witnessed by their supervisor. The IT staff will then submit the signed form to Human Resources after the account has been created and activated to keep with their personnel file. This form is

also used for student account creation, and after the account has been created the students are allocated a default level of security.

Temporary passwords are initially issued and the user will be prompted to change the password immediately after the first successful login. The password complexity outline is:

a) Minimum of 7 characters;
b) Must contain letters and numbers only;
c) Must contain at least one capital and lower case letter along with a number;
d) Cannot contain the user's name, previous passwords, or any illegal characters;
e) Passwords will expire every 60 days; the user will be prompted before this time to change to a new password. The system will track the last 24 passwords used to ensure no duplication occurs;
f) Passwords will only be transmitted in person to staff members or via college email address. Passwords will not be sent to personal email addresses, and only over the phone in situations where the I.T. Department is able to correctly identify the requester beyond any doubt.

The authorization procedure for determining who is allowed to access which network and networked services is documented using the Service Desk software from the initial point of contact (service request submission) to its conclusion. This information is available to the requestor, and stored in the Service Desk system for future use if required.

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 with 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 service ticket request submission.

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 mandatory screen lock timers.

G.7.01.05 Network Access

Network access required by staff is requested by supervisory staff to IT using the Service 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 Outlook Web Access using an internet browser, or remote desktop for network file access. Both methods require an active college user account and password to access, and the individual can only access areas in which they have permission to do so.

G.7.01.06 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 direct supervisor will notify the IT Staff (via Service Tickets) and Human Resources immediately to either remove network access by deactivating the account or adjust 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 supervisor 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.

G.7.01.07 Virus and Malware Log Review

Security logs from the Symantec server are transmitted to the IT Department who will then review 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.

G.7.01.08Physical 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 Director of Finance & Administration, Director of the North at the Meadow Lake campus, the IT staff members, and the Facilities Department staff. Non-IT staff may only access these areas under direct permission and supervision of IT or the Director of Finance and 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 IT Coordinator.

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 with locking

cables 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.

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. (e.g. server rooms, network cabling locations, etc.) These areas must remain secure at all times.

Equipment will be catalogued into inventory when received along with information about the hardware and its intended location. These records are maintained to allow for proper equipment tracking and inventory. 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 (e.g. 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 department 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.

G.7.01.09 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.

G.7.01.10 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.

G.7.01.11 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 Symantec Enterprise Manager). 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 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 Director of Finance and 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.

G.7.01.12 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.

G.7.01.13 Data Backup and Recovery

Server data is stored on the Network-Attached Storage (NAS) devices located at the North Battleford and Meadow Lake locations. These devices contain all the network data from their respective campus as well as back up files from each other's campus. All server and network data is backed up to these devices locally, and copied to their partner campus. This provides a redundant and off site data backup. This occurs using the CommunityNet (CNet) internet connections provided by the Ministry of Education using a secure Virtual Private Network (VPN) tunnel. The purpose of this process is to allow for file, server, and site recovery as outlined in the disaster recovery plan.

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 IT Coordinator 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 Director of Finance and 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 Director of Finance and Administration and documented in the Service Desk software for historical reference.

Information security continuity is addressed through the College business continuity planning. All college staff is responsible for protecting information within reasonable expectations according to the event (i.e. natural disasters, accidents, equipment failure, and deliberate actions). These risk scenarios are identified in related documents (i.e. DRP, ERP, etc.) as they identify the critical business processes and continuity requirements relating to operations, staffing, materials, transport and facilities in the event of a crisis and will be reviewed on an ongoing basis.

G.7.01.14 Change Management

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

All changes to the North West College production environment will be tracked via a Service Request ticket. Service requests will be entered into and managed via the Service Desk Ticketing System 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 IT Coordinator prior to execution to ensure a proposed change does not compromise the stability of the production environment.

Changes to the production environment are:

a) Implemented using the appropriate Change Management Process.
b) Documented using the Service Desk System.
c) Approved by the IT Coordinator during Standard Changes and Immediate Changes.
d) Communicated effectively that all responsible parties are aware of the change assignment and all user communities are aware of any potential impact.

The IT Coordinator (or IT Technician in collaboration with the Director of Finance and 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 Director of Finance and Administration for further approval at a management level.

Computer Software Information Technology 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, mobile lab computer carts, and staff loaner laptops (Referred to as lab computers from this point forward unless specified). Specialized Software installation requests In order for specialized software to be installed in computer lab computers, staff will follow and be aware of the following procedures and processes.

a) Staff members will provide IT the following information:
i) License information regarding the software
ii) A copy of the software installation media. Installation instructions no later than 45 days prior to the start of the fall, spring, or summer semester. The IT staff will maintain a copy of the license information and software installation media. Software purchase requests are to be submitted to the IT Service Desk and from there will be reviewed for approval and pricing if required. The information will then be communicated back for purchase.

b) IT will install, test, and document the installation of the software on a computer designated as a testing computer (either physical or virtual) and ensure that the software does not conflict with any other installed software. Staff will be contacted during the 45 day period and asked to test the software application in order to ensure that it will work properly for his/her class.

c) If the application testing is successful it will be installed on the computer lab computers prior to the beginning of the semester. The IT staff will contact the instructor and/or department if there are issues.

d) Pre-existing specialized software will be automatically installed in lab computers every semester until the staff member requests that it be removed

or the license has expired for the software, if applicable. Staff will not have to request the re-installation of same specialized software every semester unless an updated version is available and needed. At which time it is their responsibility to notify IT of the change and what is required to acquire the new version.

e) The staff member that initially requested the software installation, and their direct supervisor, will be the contacts if the IT staff members need to consult with the staff member regarding the software.

f) Staff must submit an IT Service Desk ticket prior to considering using or purchasing software that they intend to use on a computer lab computer. Software purchases must be approved by IT. Proper licensing must be purchased to ensure that software will be installed on every computer required (e.g. the entire computer lab, set of classroom computers, or instructor station). The IT staff members will be able to assist with decisions regarding software purchases, as well as consult approved software vendors for additional information and pricing.

g) It will be understood that if a staff member requests that specialized software be installed after the 45 day testing period or during the semester, IT may not be able to accommodate the request in a timely manner.

h) A list of installed software will tracked by IT for future reference for building and testing purposes. Specialized software updates and upgrades:
   i) Software updates are patches or additions to pre-existing specialized software. If the IT staff members discover that some updates have become available for specialized software, they will inform faculty that there are updates available. The update(s) will be installed on a test computer so that the faculty member can test the software. If both staff agrees to install the update(s), IT will install the update on the lab computers as required. It should be noted that depending on the complexity of the update, and the limited access to computer labs, it may take up to two weeks to install the update(s).
   ii) Software upgrades are new versions of pre-existing specialized software. If a software upgrade is made available, a Service Desk installation request must be submitted to IT. Software and Operating System Installation Procedures
   iii) Computer lab imaging consists of copying a complete installation of standard and specialized software and operating systems to a lab computer. This process erases all data stored on a computer and replaces it with a clean' image. Any information is erased it will be not be retrievable.
   iv) Lab computers will be imaged prior to the beginning of the fall semester; if the need arises, the lab computers can be imaged at any time. IT will try to ensure that lab services are not interrupted due to the imaging process.

v) The College computer lab image will be updated at a minimum of once a year. A computer will be setup with the new software image for IT to test and ensure that specialized and standard software is functioning satisfactorily.
vi) IT maintains the installation and setup procedure documentation for specialized and standard computer lab software and operating systems. The documentation regarding the system setup will be available to faculty if they request it.
vii) IT will help ensure that all lab computers receive all critical operating system and virus system updates in a timely fashion.

G.7.01.15 Legislative and Contractual Compliance

Supervisors 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.

G.7.01.16 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 "Computer Use Policy and Procedural Guidelines Acceptable Use Agreement (per Policy 3.03)" in which all users both staff and student are required to review and sign prior to being granted an account. Further information involving user access security can be found in Procedure 1.20.3 User Access Controls and Authorization.

* * *

PROCEDURE G 7.03

Subject: **Cell Phone**

Approval/Amendment Date(s): August 16, 2016

Associated Procedure/Documents: Policy 7.03 Cell Phone

Next Review Date:

G.7.03.01

Cell phones requests must be provided in writing and signed off by the CEO or Director responsible.

G.7.03.02

Cell phones purchased will be at a cost of $0 and must be one of the models suggested by the Coordinator of IT. Any deviation away from the $0 cost, must be approved by the Director and the cost of the purchase will be coded to the applicable responsibility center.

G.7.03.03

All cell phone devices will be on a two year contract.

* * *

PROCEDURE G 7.04

Subject: **Records Retention and Disposal**

Approval/Amendment Date(s): December 5, 2019

Associated Procedure/Documents: Policy 7.04 Records Retention and Disposal

Next Review Date:

Procedures:

G.7.04.01

All responsibility centres of the College shall ensure records are retained for the period of time set out in the Records Retention Schedule.

G.7.04.02

Each responsibility centre is responsible for the ongoing process of identifying its records which have met the required retention period and recommending destruction thereof.

G.7.04.03

The retention periods referred to in the Records Retention Schedule relate only to records in paper form.

G.7.04.04

Any document not listed in the Records Retention Schedule shall be retained for a period of seven (7) years from date on which it was created unless any one or more of them should be retained for archival purposes.

G.7.04.05

Permission for the destruction of records must be given by the Director of Finance and Administration or Director of Programs prior to their destruction.

G.7.04.06

When records have been identified as those to be destroyed, and permission to do so has been given by the Director of Finance and Administration or Director of Programs, the records are to be shredded or identified for Confidential Recycling.

G.7.04.07

Where records are to be kept permanently, duplicate records of any kind, not used as working copies, shall be eliminated keeping only the original.

G.7.04.08

A record of all files destroyed must be retained with a copy provided to Administration.

G.7.04.09 Attachment(s):

a) Attachment A: Records Retention Schedule

* * *

G.7.04.09 ATTACHMENT A
RECORDS RETENTION SCHEDULE

SIX (6) months	Applications/Resumes for Employment
ONE (1) year	Correspondence, General: e.g., congratulations, greetings, etc. Job resumes for posted positions/Interview Notes
TWO (2) years	Agendas Day Files Insurance Policies – Expired
FIVE (5) years	Correspondence, General Correspondence, Public Relations Detailed Budget Working Papers Equipment Inventory Records Purchasing Documentation (Purchasing, Receiving & Stores)
SEVEN (7) years	Accident Reports Bank Deposit Books/Bank Statements Bills of Lading Bond Applications Budgetary Information Capital Project Documentation Correspondence, Special Projects and tenders Donation Receipts Employee Records (after termination) Expense Reports Federal Income Tax Returns Insurance – Disability and Pension Insurance Policies – Property, Liability, etc. Inventories Year-end Job Postings Legal Correspondence, Agreements, Contracts, (after expiration) Miscellaneous Contracts and Agreements (after expired) Payroll Data – Part-time employees (after termination) Purchase Orders Asset Requisitions Research Projects Safety and Occupational Health Correspondence Scholarships, Bursaries Source Documentation – Invoices, Sales Summaries, AJEs Student Loans Student Medical Records

	Sick Leave Reports
PERMANENT RECORD	Annual Reports Archival Information Audited Financial Statements Board Minutes Bylaws Collective Agreements Committee Minutes Construction Projects in Excess of $50,000 Course Calendars Credit Course Outlines Ledgers and Journals Legal Deeds and Leases Mission and Goals Statements Pension/Superannuation Reports Permanent Student Record Files Personnel Files (active employees) Property Documentation Records of Files Destroyed

* * *

PROCEDURE G 7.05

Subject: **BACKUP**

Approval/Amendment Date(s): January 6, 2022

Associated Procedure/Documents: Policy 7.05 Backup

Next Review Date:

Procedures:

G.7.05.01 *Backup Retention*

Retention Period

Backups of all data must be retained such that all systems are fully recoverable. At a minimum, each full backup weekly must be retained for 5 weeks and a full monthly backup for 13 months.

The retention period and any requirement for archive copies to be retained for longer periods (or permanently) must be formally determined for critical business information as well as based on any legal requirements.

G.7.05.02 *Backup Documentation*

Backup documentation must include identification of all critical data, programs, documentation, and support items that would be necessary to perform essential tasks during a recovery period.

Each backup media must be appropriately labeled with a record of details including the date and nature of the backup (e.g. Full image copy or file copy) in an appropriate log.

Any backup media to be physically transported from College to the offsite location must be logged.

The on-site backup media log must contain the following information:

- Date of taking the backup.
- Date of transporting/copying the media to the offsite location
- Contents of the media (e.g. transaction backup, application backup, entire system backup)
- Nature of backup (e.g. full, incremental, or file copy)

Documentation of Restoration Process

Documentation of the restoration process must include procedures for the recovery from single-system or application failures as well as for a total North West College Data Center disaster scenario.

Review of Documentation

Backup and recovery documentation must be reviewed and updated annually to account for new technology, business changes, and migration of applications to alternative platforms. The volume of data that is modified over a certain time period must be considered while establishing the frequency of data backup. This includes the application and operational software, system data (e.g. initialization files, macro definitions, configuration data, text blocks, password files, access-right files), the application data as such and the protocol data (such as that relating to log-ins and data transmissions).

Specifying the Data to be Backed up

Where data is modified continuously in a system, an appropriate data backup frequency must be specified based on modification, availability, integrity and critical business information.

Data Availability Requirements of the IT Applications

A proven standard like the maximum permissible downtime specifies the time period during which the specialized task can be performed without the availability of the relevant data and without the need for resorting to backup copies. Consideration must also be given as to whether paper usage would allow short- term continuation of operations without IT support.

Effort Required for Data Reconstruction Without Data Backup

It must be known whether, and how easily, destroyed databases can be reconstructed if backup data were not available.

The sources from which the data could be reconstructed must be examined and documented.

Deadlines

It must be determined whether certain deadlines have to be observed for the data. This can involve storage or deletion deadlines relating to person-related data.

These deadlines must be considered when laying down the system specific data backup policies.

Confidentiality Requirements

Consideration must be given as to the confidentiality requirements of the data needing backup or restoration. On restoration all security and user rights must be maintained

Integrity Requirements

Data backups must ensure that data are stored integrally and not modified during the period of storage.

Secondary Backup Copy Requirements

A copy of backups shall be transmitted to the opposing campus after the backup has completed. This copy shall be kept secure from any tampering or copying and shall only be used by the IT Coordinator to recover data in event of a catastrophe.

Knowledge and Data-Processing Competence of IT Users

Only College Technicians or System Administrator with the requisite skills and capabilities must be allowed to carry out data backups and/or restores.

Planning Backup and DR levels

Rate 1 to 5 total 15

Folder or Share	Confidentially 5 very confidential	Business Critical 5 most critical	time/changes can loose 5 being none	Total Level 15 highest

Data Source BACKUP Manifest

Date:	Server Name:
Share/Drive:	Level:

List of Files/Folders to be Backed Up

Backup Client and Policy

Backup Client Installed On Client Server:	

Only One Full(F) followed by either a Differential(D) or an Incremental(I)

Backup Policy for Client Server:	**daily**	**weekly**	**monthly**
Monday	I	F	F
Tuesday	I	F	F
Wednesday	I	F	F
Thursday	I	F	F
Friday	I	F	F
weekend	NONE	none	NONE

Retention and Offsite

Retention Period for Backup:	X years			Months
Offsite Storage:	WHERE	DATE	Signed	

Requestor's Signatures_____ Date:_____

Backup Administrator _____Date:_____

* * *