Approved by Council

April 1, 2015

Executive Summary
Saskatchewan College of Paramedics
Risk Management Compliance Document

The primary purpose of this document is to ensure that the Saskatchewan College of Paramedics (SCoP) establishes appropriate standards for operational security and risk management.

In situations where existing SCoP policy is identified as failing to meet minimum acceptable standards, additional requirements have been added and amendments to SCoP documents incorporated into new and existing organizational policy.

This compliance document provides a framework perspective of SCoP security policy, more specifically as it relates to data management and protection within a predominantly technology based environment. The principles found within the document serve to guide the development and implementation of Information Technology security policy moving forward. These principles represent a standard for data protection that has been adopted internationally by the payment card industry (PCI DSS V3.0), which in general, defines standards and levels of protection that meets or exceeds minimum standards currently required by the health professional regulatory industry in Saskatchewan.

The SCoP compliance document is based upon the following basic principles for security:

Principle	Outputs and Outcomes
Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Organizational Data	**3.** Protect stored data **4.** Encrypt transmission of member data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to confidential data by business need to know **8.** Identify and authenticate access to system components **9.** Restrict physical access to member data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and member data **11.** Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

Policy Framework Management

Current SCoP security requirements and guidelines are embedded in existing organizational policy documentation and applicable legislation. Where available, existing policy and guidelines will be referenced within the SCoP Risk Management Compliance document and attached as appendices.

SCoP Compliance Document (New):

The SCoP Risk Management Compliance document has been divided into a number of sections, each representing a potential security risk area.

As SCoP does not currently have formal security specific policies in place, the Risk Management Compliance document will establish a foundation upon which more specific privacy and security policy documents and standards references can be appended. In total, these documents will form an overarching "Risk Management" and "Privacy and Security" policy framework for the organization.

The following policy sections have been identified as foundational to appropriate risk management:

1. Acceptable Use Policy Link to Section
2. Password Policy Link to Section
3. Remote Access Policy Link to Section
4. Confidential Data Policy Link to Section
5. Mobile Device Policy Link to Section
6. Retention Policy Link to Section
7. Email Policy Link to Section
8. Backup Policy Link to Section
9. Network Access and Authentication Policy Link to Section
10. Incident Response Policy Link to Section
11. External Connection Policy Link to Section
12. Wireless Access Policy Link to Section
13. Network Security Policy Link to Section
14. Encryption Policy Link to Section
15. Outsourcing Policy Link to Section
16. Physical Security Policy Link to Section

Section I: Acceptable Use Policy

The Saskatchewan College of Paramedics is hereinafter also referred to as "SCoP" or "the College"

1.0 Overview

Every employee will ensure that corporate resources (including information technology "IT") are used appropriately and in a manner that does not compromise the confidentiality of proprietary or other sensitive information, nor bring embarrassment or criticism to SCoP.

Limited incidental personal use of corporate resources for personal reasons will be permitted providing that it follows the provisions in this policy, does not interfere with the employee's regular duties or those of other employees, and does not hinder computer system performance. The cost of such personal use (e.g. long distance telephone charges) will be borne by the employee.

Employees will take reasonable and necessary measures to safeguard the operating integrity of technology systems and their accessibility by others. Additionally, individuals will perform their jobs in accordance with all applicable laws, regulations and policies. Specific SCoP policies (or relevant legislation) will also apply to those using the SCoP information technology infrastructure. These references include:

- *The Paramedics Act;*
- *Personal Information Protection and Electronic Documents Act;*
- *The Health Information Protection Act*;
- SCoP corporate policies and procedures including those respecting harassment, performance improvement, code of conduct, conflict of interest, and corrective discipline.

Violation of this policy will be subject to corrective discipline up to and including possible dismissal.

2.0 Purpose

Since inappropriate use of corporate systems exposes SCoP to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of corporate resources for the protection of all parties involved.

3.0 Scope

SCoP is committed to providing an environment that encourages the use of computers and electronic information as essential tools to support the SCoP mandate.

For the purposes of this policy, information technology includes computer hardware, software, the Internet, email, telephones, voice mail, cellular phones, PDAs, fax machines and photocopiers.

This policy applies to all SCoP employees and those working under contract to SCoP who use any information technology resources which:

- Are owned, licensed or leased by SCoP;
- Connect directly to SCoP data or telephone networks;
- Connect directly to a computer or other device owned or operated by SCoP; or
- Otherwise use or affect the SCoP information technology infrastructure.

The files of SCoP employees (paper or electronic, including email) may be subject to subpoena in legal proceedings.

All information stored on SCoP equipment is the property of SCoP; employees should have no reasonable expectation of privacy. While SCoP respects the confidentiality of information stored and transmitted on its networks and computers, the organization reserves the right to monitor information technology use, and to access the contents of all stored files and messages transmitted on its information technology infrastructure. Employees should be aware that computer usage can be traced and is also routinely reviewed for purposes of capacity planning, security management and policy compliance.

Like any other corporate asset, information technology is intended for use to conduct corporate business. However SCoP recognizes that employees may occasionally use information technology resources for personal reasons. SCoP reserves the right to determine what constitutes incidental use.

Since the confidentiality of electronic media cannot be guaranteed, employees are expected to exercise caution and good judgment when committing sensitive information to storage or transmission on any electronic media.

4.0 Policies

4.1 Network Access

As the user will be given access to the corporate network, Internet, and other IT resources, SCoP expects the user to use these resources in a responsible manner.

The user must make a deliberate effort to avoid accessing network data, files, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access.

4.2 Web Browsing and Internet Usage

The Internet is a network of interconnected computers of which the SCoP has very little control. The user must recognize this when using it, and understand that as a public domain, they may come into contact with information that is offensive, sexually explicit, or inappropriate, or that may be illegal in some jurisdictions. The user must access the Internet at his or her own risk. SCoP is not responsible for any information that the user views, reads, or downloads from the Internet.

4.2.1. Personal Use

SCoP recognizes that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of company computer systems to access the Internet is permitted as long as such usage follows the "Personal Use" policies detailed in this document, and does not have a detrimental effect on SCoP or on the user's job performance.

4.2.2 Streaming Media

Streaming media can use a great deal of network resources and thus must be used carefully. Reasonable use of streaming media is permitted as long as it does not negatively impact the computer network or the user's job performance.

4.2.3 Blogging

Blogging by SCoP employees is subject to the terms of this policy, whether performed from the corporate network, personal systems, or other external systems. The user is asked to recognize that information posted on a blog immediately becomes public information and thus to exercise extreme discretion in the type of information posted.

Users must adhere to corporate and legislated disclosure requirements at all times. In no blog or website, including blogs or sites published from personal or public systems, should internal company business matters be discussed, confidential data released, or material detrimental to the College published.

4.2.4 Instant Messaging

The user should recognize that instant messaging technology, unless specific encryption measures are taken, is an insecure medium and should take any necessary steps to follow guidelines on disclosure of confidential data. Unencrypted confidential data must never be sent via instant messaging technologies. Member credit card/primary account numbers (PANs) must never be sent via instant messaging, regardless of encryption.

4.2.5 Bandwidth Usage

Excessive use of company bandwidth or other computer resources, where not required by job function, is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low company-wide usage. SCoP may restrict bandwidth for certain services deemed non-critical to company operations, or as it sees fit to preserve network functionality.

4.2.6 Social Networking/Social Media

One of the benefits of the Internet is the ability to engage in public discussion groups. However, whenever a SCoP user participates in a public discussion and posts messages that are seen to be from SCoP, anything that is written will reflect on the organization.

When joining in public discussion on-line, users must identify whether they are participating as an individual or as a representative of the College. Whenever a user engages in a public discussion through a SCoP account or is identified as being from SCoP, all messages must conform to College standards of accuracy, courtesy and propriety.

Employees must recognize that information posted on social networking sites is public information and to exercise extreme discretion in the type of information posted. Confidential information must not be posted on social networking sites. Further, the user should restrict his or her privacy settings to the fullest extent possible. Users must not publish any information detrimental to the College.

In most cases, it is appropriate to participate in on-line discussions as an individual rather than as a representative of SCoP. When posting messages on behalf of SCoP, employees should have all messages reviewed by the Executive Director before posting. A disclaimer should be included where practical, but does not reduce the employee's responsibility for ensuring that standards are met.

As long as company policies are followed, SCoP allows reasonable use of social networking sites from its network and/or during business hours. This use must either be business related, or consume no more than a trivial amount of the user's time and network resources. The employee assumes all risks associated with social networking.

4.3 Unacceptable Use

The following actions shall constitute unacceptable use of the corporate network. This section is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable.

4.3.1 Prohibited Actions

The user may not use the corporate network and/or systems to:

- Engage in activity that is illegal under local, provincial, federal, or international law;
- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the College;
- Download, store, or distribute violent, perverse, obscene, lewd, or offensive material;
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media;
- Engage in activities that cause an invasion of privacy and/or compromise privacy legislation or policy;
- Engage in activities that cause disruption to the workplace environment or create a hostile workplace; and
- Reveal personal or network usernames or passwords to others.

4.3.2 Circumvention of Security

Using company-owned or company-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or the escalation of privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent company security systems is expressly prohibited. This includes disabling or tampering with any company supplied security software, such as antivirus/anti-malware software or remote access software.

4.3.3 Use for Illegal Activities

No company-owned or company-provided computer systems may be used for activities that are considered illegal under local, provincial, federal, or international law. Such actions may include, but are not limited to, the following:

- Unauthorized port scanning;
- Unauthorized network hacking, including: packet sniffing, port scanning, packet spoofing, wireless hacking, etc.;
- Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system;
- Acts of terrorism;
- Cybercrime, extortion, or identity theft;
- Downloading, storing, or distributing any material prohibited by law;
- Downloading, installing, or distributing unlicensed or "pirated" software; and
- Sending unsolicited bulk email or other messages deemed illegal under applicable regulations.

SCoP will take all necessary steps to report and prosecute any violations of this policy.

4.3.4 Overuse

Actions detrimental to the computer network or other corporate resources, or that negatively affect employee job performance, are not permitted.

4.3.5 Copyright Infringement

SCoP computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of the Acceptable Use Policy, if done without permission of the copyright owner:

a) Copying and sharing images, music, movies, or other copyrighted material using person to person (P2P) file sharing or unlicensed CD's and DVD's;
b) Posting or plagiarizing copyrighted material; and
c) Downloading copyrighted files which employee has not already legally procured.

Employees will photocopy copyright-protected works only in accordance with the provisions of the *Copyright Act of Canada*. This list is not meant to be exhaustive, copyright law applies to a wide variety of works and applies to much more than is listed above.

4.4 Monitoring and Privacy

Users should expect no privacy when using the corporate network or company resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The College reserves the right to monitor any and all use of the computer network. To ensure compliance with company policies this may include the interception and review of any emails, or other messages sent or received; inspection of data stored on personal file directories, hard disks, and removable media; and monitoring of Internet/network usage.

4.5 Responsible Computer and Network Use

SCoP expects users to utilize the network responsibly. Personal usage of company computer systems is permitted as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on the College or on the user's job performance.

4.5.1 Non-Company-Owned Equipment

Non-company-provided computer equipment is expressly prohibited from being connected to the SCoP network without the necessary approval(s).

4.5.2 Removable Media

Personal (non-company-owned) storage devices represent a serious threat to data security and are expressly prohibited from being connected to the SCoP network without approval.

4.5.3 Software Installation

Installation of non-company-supplied software applications is prohibited to prevent the inadvertent introduction of security threats through malware, spyware, Trojans etc.

4.6 Reporting of a Security Incident

In the event a security incident or breach of any security policies is discovered or suspected, the user must immediately follow any applicable guidelines as detailed in the corporate incident response policy.

4.7 Applicability of Other Policies

This document will form part of the College's cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as necessary.

5.0 Enforcement

All users are subject to and must comply with this document, SCoP Policy Manual and Code of Conduct, *The Paramedics Act*, *The Health Information Protection Act* (HIPA) and all other applicable legislation and bylaws.

SCoP policies outline corrective and/or disciplinary options for non-compliance. All incidents will be investigated where results and findings could be used as part of disciplinary, contract review or legal actions.

Section II: Password Policy

The Saskatchewan College of Paramedics is hereinafter also referred to as "SCoP" or "the College"

1.0 Overview

A solid password policy is one of the most important security controls an organization can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy is essential so that all users understand that they are responsible for protecting system and network passwords. This includes passwords for all computers, laptops, mobile devices etc. and SCoP equipment.

2.0 Purpose

The purpose of this policy is to specify guidelines for use of passwords. This is to protect the confidentiality, security and integrity of corporate information that is accessed and stored on SCoP equipment from unauthorized use. Importantly, this policy will help users understand why strong passwords are a necessity, and help them create passwords that are both secure and useable.

3.0 Scope

This policy applies to every individual who is provided an account on the College network or systems, including: employees, guests, contractors, partners, vendors, etc.

4.0 Policies

4.1 Construction

SCoP must ensure that password construction standards are in place for user reference. Passwords must have both complexity and strength and meet a minimum set of standards regarding length and a mix of numeric and alphabetic characters.

In addition, it is important that SCoP mandate that users adhere to the approved standards regarding construction of passwords, which must reflect minimum industry standards or greater.

4.2 Confidentiality

Passwords are considered confidential data and treated with the same discretion as any of the organization's proprietary information. They must be safeguarded from detection by any unauthorized person, and must not be disclosed, shared, left in unsecured in open spaces, recorded, saved on applications, reused or included in emails or other correspondence.

4.3 Change Frequency

In order to maintain good security, passwords must be changed on a regularly scheduled basis. This limits the damage an attacker can do, as well as helps to frustrate and slow attempts to crack a password through brute force. At a minimum, the College must require users to meet industry standards on change frequency, or 90 days whichever is shorter. Users must not reuse the same password as the previous four.

4.4 Incident Reporting

Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to the person responsible for network security and immediately change the password in question. Any request for passwords over the phone or email, whether the request came from organization personnel or not, must be expediently reported. When a password is suspected to have been compromised the responsible security manager will request that the user, or users, change all of his or her passwords.

4.5 Applicability of Other Policies

This document will form part of the SCoP cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies must be reviewed as necessary.

5.0 Enforcement

All users are subject to and must comply with this document, SCoP Policy Manual and Code of Conduct, *The Paramedics Act*, *The Health Information Protection Act* (HIPA) and all other applicable legislation and bylaws.

SCoP policies outline corrective and/or disciplinary options for non-compliance. All incidents will be investigated where results and findings could be used as part of disciplinary, contract review or legal actions.

Section III: Remote Access Policy

The Saskatchewan College of Paramedics is hereinafter also referred to as "SCoP" or "the College"

1.0 Overview

In the day to day operation of the organization, it is often necessary to provide access to corporate information resources for employees or others working outside the SCoP network. While this can lead to productivity improvements it can also create certain vulnerabilities if not implemented appropriately. The goal of this policy is to provide the framework for secure remote access implementation.

2.0 Purpose

This policy is provided to define standards for accessing corporate information technology resources from outside the network. This includes access (for any reason) from the employee's home, remote working locations, while traveling, etc. The purpose of this policy is to define criteria for the protection of information assets when using an insecure transmission medium. Further, the policy is also intended to ensure that processes and standards are in place respecting remote access for users based on a business need.

3.0 Scope

The scope of this policy covers all employees, contractors, and external parties that access SCoP resources over a third-party network, whether such access is performed with SCoP-provided or non-SCoP-provided equipment.

4.0 Policies

4.1 Remote Access Client Software

SCoP will supply users with remote access software that allows for secure access when outside the network and enforces the remote access policy. The software will provide strong traffic encryption in order to protect the data during transmission.

For the purpose of this policy, ownership of the remote device is irrelevant. If the device ever connects to the SCoP network this policy applies to that device.

4.2 Remote Network Access

Remote network access can be provided for a variety of reasons to a variety of different types of users. Rather than take a "one size fits all" approach, SCoP requires that remote access be offered according to the level of access required by each user type.

4.3 Idle Connections

Due to the security risks associated with remote network access, it is a good practice to dictate that idle connections be timed out periodically. The SCoP "time out" policy must meet minimum industry standards or greater.

4.4 Prohibited Actions

Remote access to corporate systems is only to be offered through an SCoP approved means of remote access. If data storage is authorized on remote computers and that data contains member information, that device and its environment and usage, must comply with applicable SCoP Security Standard requirements.

4.5 Use of Non-Company-Provided Systems

Accessing the SCoP network through home or public systems presents a security risk, as the College cannot completely control the security of the system accessing the network. User owned computers are only allowed to access the corporate network with the authorization of SCoP.

5.0 Enforcement

All users are subject to and must comply with this document, SCoP Policy Manual and Code of Conduct, *The Paramedics Act*, *The Health Information Protection Act* (HIPA) and all other applicable legislation and bylaws.

SCoP policies outline corrective and/or disciplinary options for non-compliance. All incidents will be investigated where results and findings could be used as part of disciplinary, contract review or legal actions.

Section IV: Confidential Data Policy

The Saskatchewan College of Paramedics is hereinafter also referred to as "SCoP" or "the College"

1.0 Overview

Confidential data is data that often holds significant value to a company and to others. As such, it can carry greater risk than general company data in terms of loss – both of data and/or data integrity. Provincial and Federal legislation and industry standards typically specify how certain types of data must be managed. In order to meet these mandatory standards, it is essential for organizations to define security standards that relate specifically to confidential data.

2.0 Purpose

The purpose of this policy is to detail how to identify and handle confidential data. This policy lays out standards for the classification and use of confidential member information, and outlines specific security controls to protect this data.

3.0 Scope

The scope of this policy covers all SCoP confidential data, regardless of location. Also covered by the policy are hardcopies of data, such as printouts, faxes, notes, etc.

4.0 Policies

4.1 Data Classification

Information assets are as significant (or more) to SCoP as physical property. In order to determine the value of the asset and how it should be handled, data must be classified according to its importance to operations and the confidentiality of its contents. Once this has been determined, SCoP can take steps to ensure that data is treated appropriately.

Of particular concern is confidential data and member data. This should be identified and inventoried in all its forms – electronic, printed, or stored on digital media – and

segregated from non-confidential data so that access to it can be more tightly controlled and tracked. Any media that contains member data must be catalogued and secured.

4.2 Treatment of Confidential Data

Controls for physically securing confidential data are needed to prevent unauthorized persons from accessing confidential information. Confidential data sources must be readily identified as sensitive and steps taken to ensure the security of such data. SCoP must have strict requirements in place regarding the storage, transmission, and destruction of this data.

4.2.1 Storage

Please refer to the attached procedure page regarding storage standards.

4.2.2 Transmission

Please refer to the attached procedure page regarding transmission standards.

4.2.3 Destruction

Please refer to the attached procedure page regarding destruction standards.

4.3 Examples of Confidential Data

The following list is not intended to be exhaustive, but provides guidelines on what type of information is typically considered confidential. Confidential data can include:

- Credit card information/cardholder data;
- Employee or member social insurance numbers, or other personal information;
- Medical and healthcare information;
- Personal Health Information (PHI) – in any format;
- Customer data, including customer lists and customer contact information;
- College financial data which has not been released publicly;
- Passwords;
- Bank account information and routing numbers;
- Confidential credit card data held for a third party.

4.4 Use of Confidential Data

A successful confidential data policy is dependent on the users knowing and adhering to SCoP standards involving the treatment of confidential data. The following applies to how users must interact with this data:

- Users should be aware/advised if they have been granted access to confidential data; such data should be designated/marked "confidential".
- Users must only access confidential data to perform his/her job function.
- Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information.
- Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary and only if the action is approved by the immediate supervisor.
- Users must report any suspected misuse or unauthorized disclosure of confidential information immediately to the immediate supervisor.

4.5 Sharing Confidential Data with Third Parties

If confidential data is shared with third parties, such as service providers, a written agreement must govern the provider's use of the information.

4.6 Receiving Confidential Data from Third Parties

If SCoP receives or in any way handles confidential data for other entities, such as customers or partners, it must treat this data as if it were its own confidential data. SCoP must acknowledge this responsibility through a formal agreement with the other entity.

SCoP must take all necessary steps to secure any data that it possesses, stores, processes, or transmits on behalf of its customers or partners that may affect the security of the entity's data environment.

Shared hosting providers must protect each entity's hosted environment and data. SCoP must ensure that these providers meet any industry requirements that are specific to shared hosting providers.

4.7 Security Controls for Confidential Data

Confidential data requires additional security controls in order to ensure its integrity including encryption, network segmentation, physical security, and processes covering normal business practices such as printing, email, fax, and mail. SCoP must ensure that it has processes and standards in place to meet this requirement.

4.8 Emergency Access to Data

If SCoP confidential data has critical business or health implications (i.e., personal health information), a procedure for accessing this data during an emergency must be developed and documented. SCoP must establish a procedure for emergency access in case the normal mechanism for access to the data becomes unavailable or disabled due to system or network problems.

The procedure must address the following questions:

- What process must be followed to activate the emergency access procedure?
- What systems will it involve?
- In what situations should it be activated?
- Will it be activated automatically if certain conditions are met, or will it require human intervention? If so, who is authorized to make the decision to implement the procedure?
- Who will be involved in the process and what roles will they perform?

5.0 Enforcement

All users are subject to and must comply with this document, SCoP Policy Manual and Code of Conduct, *The Paramedics Act*, *The Health Information Protection Act* (HIPA) and all other applicable legislation and bylaws.

SCoP policies outline corrective and/or disciplinary options for non-compliance. All incidents will be investigated where results and findings could be used as part of disciplinary, contract review or legal actions.

Section V: Mobile Device Policy

The Saskatchewan College of Paramedics is hereinafter also referred to as "SCoP" or "the College"

1.0 Overview

Generally speaking, a more mobile workforce is a more flexible and productive workforce. For this reason, business use of mobile devices is growing. However, as these devices become vital tools to the workforce, more and more sensitive data is stored on them, and thus the risk associated with their use is growing. Special consideration must be given to the security of mobile devices.

2.0 Purpose

The purpose of this policy is to specify SCoP standards for the use and security of mobile devices.

3.0 Scope

This policy applies to SCoP data as it relates to mobile devices that are capable of storing such data, including, but not limited to, laptops, notebooks, tablet computers, smartphones, and USB drives. Since the policy covers the data itself, ownership of the mobile device is irrelevant. This policy covers any mobile device capable of coming into contact with College data.

4.0 Policies

4.1 Physical Security

By nature, a mobile device is more susceptible to loss or theft than a non-mobile system. SCoP must carefully consider the physical security of its mobile devices and take appropriate protective measures that include ongoing monitoring of security risk and tools available to address the issues.

4.2 Data Security

If a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defense for protecting College data. The following sections specify SCoP requirements for data security as it relates to mobile devices.

4.2.1 Laptops or Mobile Computers

At a minimum, SCoP data must be stored on devices that require a username and password or biometrics for login.

4.2.2 Smartphones/Tablets

SCoP must have standards in place regarding encryption and login passwords for use with smartphones and/or tablet devices.

4.2.3 Removable Media

This section covers any USB drive, flash drive, memory stick or other removable data storage media that could be connected to SCoP systems. If provided by the College, any data stored on these devices must be encrypted using strong encryption. Member information should never be stored on removable media regardless of encryption. SCoP data is never to be stored on personal (non-company-provided) removable media without authorization.

4.2.4 Portable Media Players

No College data can be stored on personal media players.

4.2.5 Other Mobile Devices

Unless specifically addressed by this policy, storing SCoP data on other mobile devices, or connecting such devices to College systems, is expressly prohibited. Questions or requests for clarification on what is and is not covered should be directed to the Executive Director.

4.3 Connecting Mobile Computers to Unsecured Networks

Users must not connect to any outside network without a secure, up-to-date software firewall and antivirus/anti-malware application configured on the mobile computer. Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from a home network, access provided by a hotel, an open or for-pay wireless hotspot, a convention network, or any other network not under direct control of the College.

Users must pay particular attention when connecting to public hotspots, to ensure that they are connecting to the intended wireless access point, and not a mobile hotspot set up for malicious purposes.

4.4 General Guidelines

Data stored on mobile devices must be protected to ensure confidentiality and must comply with applicable corporate policies. Corporate data is never stored on non-company-provided mobile equipment unless otherwise authorized.

4.5 Audits

SCoP should conduct periodic reviews to ensure compliance (and to inventory mobile devices) with minimum industry standards, applicable SCoP Audit Policy on Security, and Use of Information Technology Policies. An internal audit may include an examination of internet activity, applications and the content of data stored on the mobile device.

4.6 Applicability of Other Policies

This document will form part of the SCoP cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies must be reviewed as necessary.

5.0 Enforcement

All users are subject to and must comply with this document, SCoP Policy Manual and Code of Conduct, *The Paramedics Act, The Health Information Protection Act* (HIPA) and all other applicable legislation and bylaws.

SCoP policies outline corrective and/or disciplinary options for non-compliance. All incidents will be investigated where results and findings could be used as part of disciplinary, contract review or legal actions.

Section VI: Retention Policy

The Saskatchewan College of Paramedics is hereinafter also referred to as "SCoP" or "the College"

1.0 Overview

The need to retain data varies widely with the type of data. Some data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. Since this can be somewhat subjective, SCoP must have a retention policy in place, to ensure that College guidelines on retention are consistently applied throughout the organization.

2.0 Purpose

Data is a valuable commodity, but when retained excessively it can become a liability. Without a clear retention policy, the volume of data steadily grows, placing an unnecessary burden on information technology (IT) resources. The purpose of this policy is to specify SCoP guidelines for retaining different types of data.

3.0 Scope

The scope of this policy covers all SCoP data stored on College-owned, leased, and otherwise College-provided systems and media, regardless of location. Physical copies of this data (printouts, faxes, copies) are also included in the scope of this document.

Note that the need to retain certain information can be mandated by provincial, federal, and/or industry requirements and legislation. Where this policy differs from applicable regulations, the greater standard will apply.

4.0 Policies

4.1 Reasons for Data Retention

SCoP does not wish to simply adopt a "save everything" mentality. That is not practical or cost-effective, and would place an excessive burden on College resources to manage the constantly-growing amount of data.

Some data, however, must be retained in order to protect SCoP interests, preserve evidence, and generally conform to good business practices. Some reasons for data retention include:

- Litigation;
- Conduct investigation;
- Security incident investigation;
- Regulatory requirements; and,
- Intellectual property preservation.

4.2 Data Duplication

As data storage increases in size and decreases in cost, companies often err on the side of storing data in several places on the network. A common example of this is where a single file may be stored on a local user's system, on a central file server, and again on a backup system.

When identifying and classifying SCoP data, it is important to also understand where that data may be stored, particularly as duplicate copies, so that this policy may be applied to all duplicates of the information.

4.3 Retention Requirements

A company holds different types of data that are used for different purposes. SCoP must establish policy guidelines to guide retention for, at minimum, personal, operational, confidential and encrypted data.

4.4 Data Destruction

Data destruction is a critical component of a data retention policy. Data destruction ensures that the College will not get buried in data, making data management and data retrieval more complicated and expensive than it needs to be, and placing an unnecessary burden on resources.

When the retention timeframe expires, SCoP must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered.

SCoP policies must specifically direct users not to destroy data in violation of this policy. Particularly forbidden is destroying data that a user may feel is personally harmful, or destroy data in an attempt to cover up a violation of law or SCoP policy. Further, any data that may be subject to a subpoena or discovery request must not be destroyed.

SCoP must create and follow a process that on a regular basis seeks out and securely deletes data that exceeds retention requirements defined in this policy.

4.5 Applicability of Other Policies

This document will form part of the SCoP cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies must be reviewed as necessary.

5.0 Enforcement

All users are subject to and must comply with this document, SCoP Policy Manual and Code of Conduct, *The Paramedics Act*, *The Health Information Protection Act* (HIPA) and all other applicable legislation and bylaws.

SCoP policies outline corrective and/or disciplinary options for non-compliance. All incidents will be investigated where results and findings could be used as part of disciplinary, contract review or legal actions.

Section VII: Email Policy

The Saskatchewan College of Paramedics is hereinafter also referred to as "SCoP" or "the College"

1.0 Overview

Email is an essential component of business communication however it can present unique challenges due to its potential to introduce a security threat to the network. Email can also have an effect on College liability by providing a written record of communications, so having a well thought out policy is essential. This policy outlines expectations for appropriate, safe, and effective email use.

2.0 Purpose

The purpose of this policy is to detail SCoP usage guidelines for the email system. This policy will help SCoP reduce risk of an email-related security incident, foster good business communications both internal and external to the College, and provide for consistent and professional application corporate email principles.

3.0 Scope

The scope of this policy includes the SCoP email system in its entirety, including desktop and/or web-based email applications, server-side applications, email relays, and associated hardware. It covers all electronic mail sent from the system, as well as any external email accounts accessed from the corporate network.

4.0 Policies

4.1 Proper Use of Company Email Systems

Users are asked to exercise common sense when sending or receiving email from College accounts. Additionally, the following applies to the proper use of the SCoP email system.

4.1.1 Sending Email

When using a SCoP email account, email must be addressed and sent carefully. Users should keep in mind that the College loses any control of email once it is sent external to the corporate network. Users must take extreme care when typing in addresses, particularly when email address auto-complete features are enabled; using the "reply all" function; or using distribution lists in order to avoid inadvertent information disclosure to an unintended recipient. Careful use of email will help avoid the unintentional disclosure of sensitive or non-public information.

4.1.2 Personal Use

Personal usage of SCoP email systems is permitted as long as A) such usage does not negatively impact the corporate computer network, and B) such usage does not negatively impact the user's job performance.

4.1.3 Business Communications and Email

SCoP uses email as an important communication medium for business operations. Users of the corporate email system are expected to check and respond to email in a consistent and timely manner during business hours.

Additionally, users are asked to recognize that email sent from a SCoP account reflects on the organization, and, as such, email must be used with professionalism and courtesy.

4.1.4 Email Signature

An email signature (contact information appended to the bottom of each outgoing email) is required for all emails sent from the SCoP email system. At a minimum the signature must include the following information:

- User name and title;
- Organization name;
- Phone number(s);
- Fax number, if applicable; and,
- URL for corporate website.
- Privacy/confidentiality statement

Email signatures must not include personal messages (political, humorous, etc.).

4.1.5 Out-of-Office Reply

SCoP recommends the use of an out-of-office reply (where available) if the user will be out of the office for an entire business day or more. The reply must notify the sender that the user is out of the office, the date of the user's return, and who the sender should contact if immediate assistance is required.

4.1.6 Mass Emailing

SCoP makes the distinction between the sending of mass emails and the sending of unsolicited bulk email (spam). Mass emails may be useful, and is allowed with the proper approvals and as the situation dictates. The sending of spam is strictly prohibited. Please refer to the SCoP policy regarding the Canadian Anti-Spam Legislation for additional information.

It is SCoP's intention to comply with applicable laws governing the sending of mass emails. For this reason, SCoP requires that email sent to more than twenty-five (25) recipients external to the College have the following characteristics:

- The email must contain instructions on how to unsubscribe from receiving future emails (a simple "reply to this message with UNSUBSCRIBE in the subject line" will do). Unsubscribe requests must be honored immediately.
- The email must contain a subject line relevant to the content.
- The email must contain contact information, including the full physical address, of the sender.
- The email must contain no intentionally misleading information (including the email header), blind redirects, or deceptive links.

Note that emails sent to SCoP employees, existing members, or persons who have inquired about College services are exempt from the above requirements.

4.1.7 Opening Attachments

Users must use extreme care when opening email attachments. Viruses, Trojans, and other malware can be easily delivered as an email attachment. Users must:

- Never open unexpected email attachments.
- Never open email attachments from unknown sources.
- Never click links within email messages unless he or she is certain of the link's safety. It is often best to copy and paste the link into your web browser, or retype the URL, as specially-formatted emails can hide a malicious URL.

SCoP may use methods to block what it considers to be dangerous emails or strip potentially harmful email attachments as it deems necessary.

4.1.8 Monitoring and Privacy

Users should expect no privacy when using the corporate network or College resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. SCoP reserves the right to monitor any and all use of the computer network. To ensure compliance with corporate policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

4.1.9 Company Ownership of Email

Users should be advised that SCoP owns and maintains all legal rights to its email systems and network, and thus any email passing through these systems is owned by the College and it may be subject to use for purposes not anticipated by the user.

Users should keep in mind that email may be backed up, otherwise copied, retained, or used for legal, disciplinary, or other reasons. Additionally, the user should be advised that email sent to or from certain public or governmental entities will be subject to Access to Information legislation.

4.1.10 Contents of Received Emails

Users must understand that SCoP has little control over the contents of inbound email, and that this email may contain material that the user finds offensive. If unsolicited email becomes a problem, SCoP may attempt to reduce the amount of this email that the users receive however no solution will be 100% effective.

The best course of action is to not open emails that, in the user's opinion, seem suspicious. If the user is particularly concerned about an email, or believes that it contains illegal content, he or she must notify their immediate supervisor.

4.1.11 Access to Email from Mobile Devices

Many mobile devices provide the capability to send and receive email. This can present a number of security issues, particularly relating to the storage of email, which may contain sensitive data, on the device.

Users are not to access, or attempt to access, the SCoP email system from a mobile device without the permission of his or her supervisor.

Note that this section does not apply if SCoP provides the device and mobile email access as part of its remote access plan. In this case, permission is implied.

4.1.12 Email Regulations

Any specific regulations (industry, governmental, legal, etc.) relating to SCoP use or retention of email communications must be appended to this policy.

4.2 External and/or Personal Email Accounts

SCoP recognizes that users may have personal email accounts in addition to their College-provided account. The following sections apply to non-College provided email accounts:

4.2.1 Use for Company Business

Users must use the corporate email system for all business-related email. Users are prohibited from sending business email from a non-College-provided email account unless authorized.

4.2.2 Access from the Company Network

Users are permitted to access external or personal email accounts from the corporate network, as long as such access uses no more than a trivial amount of the users' time and company resources.

4.2.3 Use for Personal Reasons

Users should use a non-College-provided (personal) email account for all non-business communications. The corporate email system is for corporate communications. Users must follow applicable policies regarding the access of non-College-provided accounts from the SCoP network.

4.3 Confidential Cardholder Data and Email

SCoP must have policy covering email accounts in order to protect the security of the system, and to protect member information. This policy must be used in conjunction with policies on password, encryption, and (general) confidential data.

The following sections relate to confidential cardholder data and email:

4.4 Company Administration of Email

SCoP will use its best effort to administer the College email system in a manner that allows the user to both be productive as well as reduce the risk of an email-related security incident.

4.4.1 Filtering of Email

A strategy to mitigate risk from email is to filter it before it reaches the user so that the user receives only safe, business-related messages. For this reason, SCoP may choose to filter email at the Internet gateway and/or the mail server, in an attempt to filter out spam, viruses, or other messages that may be deemed: A) contrary to this policy, or B) a potential risk to the College information technology (IT) security. No method of email filtering is 100% effective, so the user is asked additionally to be cognizant of this policy and use common sense when opening emails.

Additionally, many email and/or anti-malware programs will identify and quarantine emails that it deems suspicious. This functionality may or may not be used at the discretion of the Executive Director.

4.4.2 Email Deletion

Users are encouraged to delete email periodically when the email is no longer needed for business purposes. The goal of this policy is to keep the size of the user's email account manageable, and reduce the resource burden with storage and backup of messages.

Please note that users are strictly forbidden from deleting email in an attempt to hide a violation of this or another College policy. Further, email must not be deleted when there is an active investigation or litigation where that email may be relevant, or if the email is the only source of an operational record.

SCoP must attach to this policy, any applicable regulations or statutes that apply to email deletion.

4.4.3 Retention and Backup

Email must be retained and backed up in accordance with the applicable policies.

4.4.4 Address Format

Email addresses should be constructed in a standard format in order to maintain consistency across the organization. The intent of this policy is to simplify email communication as well as provide a professional appearance.

4.4.5 Email Aliases

Often the use of an email alias, which is a generic address that forwards email to a user account, is a good idea when the email address needs to be in the public domain, such as on the Internet. Aliases reduce the exposure of unnecessary information, such as the address format for company email, as well as (often) the names of SCoP employees who handle certain functions. Keeping this information private can decrease risk by reducing the chances of a social engineering attack.

A few examples of commonly used email aliases are:

- office@colllegeofparamedics.sk.ca
- techsupport@companydomain.com
- info@companydomain.com

SCoP must have policy in place regarding the use of email aliases.

4.4.6 Account Activation

Email accounts will be set up for each user determined to have a business need to send and receive company email. Accounts will be set up at the time a new hire starts with the SCoP, or when a promotion or change in work responsibilities for an existing employee creates the need for email access.

4.4.7 Account Termination

When a user leaves the organization, or his or her email access is officially terminated for another reason, SCoP will disable the user's access to the account by password change, disabling the account, or another method. SCoP must have policies and procedures in place to ensure that account termination occurs in a timely manner.

4.4.8 Storage Limits

As part of the email service, email storage may be provided on SCoP network servers or other devices. The email account storage size must be limited to what is reasonable for each employee, at the determination of the Executive Director. Storage limits may vary by employee or position within the organization.

4.5 Prohibited Actions

The following actions shall constitute unacceptable use of the SCoP corporate email system. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate email system to:

- Send any information that is illegal under applicable laws.
- Email is an insecure method of communication, and thus information that is considered confidential or proprietary to the organization may not be sent via email, regardless of the recipient, without proper encryption.
- Send Credit Card Primary Account Numbers (PANs) via email, regardless of encryption.
- Access another user's email account without A) the knowledge or permission of that user - which should only occur in extreme circumstances, or B) the approval of the Executive Director or Council Executive in the case of an investigation, or C) when such access constitutes a function of the employee's normal job responsibilities.
- Send any emails that may cause embarrassment, damage to reputation, or other harm to the organization.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, harassing, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Send emails that cause disruption to the workplace environment or create a hostile workplace. This includes sending emails that are intentionally inflammatory, or that include information not conducive to a professional working atmosphere.
- Make fraudulent offers for products or services.
- Attempt to impersonate another person or forge an email header.
- Send spam, solicitations, chain letters, or pyramid schemes.
- Knowingly misrepresent SCoP capabilities, business practices, or policies.

SCoP may take steps to report and prosecute violations of this policy, in accordance with College standards and applicable laws.

4.5.1 Data Leakage

Data can leave the network in a number of ways. Often this occurs unintentionally by a user with good intentions. For this reason, email poses a particular challenge to the organization’s control of its data.

Unauthorized emailing of SCoP data, confidential or otherwise, to external email accounts for the purpose of saving this data external to company systems is prohibited. If

a user needs access to information from external systems (such as from home or while traveling), that user must notify his or her supervisor rather than emailing the data to a personal account or otherwise removing it from SCoP systems.

SCoP may employ data loss prevention techniques to protect against leakage of confidential cardholder data at the discretion of the Executive Director.

4.5.2 Sending Large Emails

Email systems were not designed to transfer large files and as such emails must not contain attachments of excessive file size. SCoP should have policy in place to limit the size of messages.

4.6 Applicability of Other Policies

This document will form part of the SCoP cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies must be reviewed as necessary.

5.0 Enforcement

All users are subject to and must comply with this document, SCoP Policy Manual and Code of Conduct, *The Paramedics Act*, *The Health Information Protection Act* (HIPA) and all other applicable legislation and bylaws.

SCoP policies outline corrective and/or disciplinary options for non-compliance. All incidents will be investigated where results and findings could be used as part of disciplinary, contract review or legal actions.

Section VIII: Backup Policy

The Saskatchewan College of Paramedics is hereinafter also referred to as “SCoP” or “the College”

1.0 Overview

A backup policy is a significant part of any corporate risk mitigation strategy. It provides the last line of defense against data loss and is sometimes the only way to recover from a hardware failure, data corruption, or a security incident. A backup policy is related closely to a disaster recovery policy, but since it protects against events that are relatively likely to occur, in practice it will be used more frequently than a contingency planning document. A company's backup policy is among its most important policies.

2.0 Purpose

The purpose of this policy is to provide a consistent framework to apply to the backup process. The policy will provide specific information to ensure backups are available and useful when needed - whether to simply recover a specific file or when a larger-scale recovery effort is needed.

3.0 Scope

This policy applies to all data stored on SCoP systems. The policy will provide standards regarding: the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures.

4.0 Policies

4.1 Identification of Critical Data

SCoP must have processes in place to identify what data is most critical to the organization. This can be done through a formal data classification process, through an informal review of information assets, or a combination of both. The object of this effort is to identify and classify data so that restoration priority can be determined.

Any data deemed confidential must be identified so that backups of this data are treated and secured accordingly.

4.2 Data to be Backed Up

A backup policy must balance the importance of the data to be backed up with the burden such backups place on the users, network resources, and the backup administrator. Data to be backed up must include:

- All data determined to be critical to SCoP operations and/or employee job function.
- All information stored on the corporate file server(s) and email server(s). It is the user's responsibility to ensure any data of importance is moved to the file server.
- All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.
- Logs and configuration information from network devices such as switches, routers, etc.

4.3 Backup Frequency

Backup frequency is critical to successful data recovery. SCoP must have policy in place that defines a regular backup schedule that will allow for sufficient data recovery in the event of an incident. Policy must meet minimum industry standards in this area as follows:

- Incremental back-up: every 3 days
- Full back-up: weekly

4.4 Off-Site Rotation

Geographic separation from the backups must be maintained, to some degree, in order to protect from natural disaster or large-scale catastrophes. Offsite storage must be balanced with the time required to recover the data, which must meet the SCoP business restoration requirements. SCoP backup media must be rotated off-site at least once per week and location security reviewed on an annual basis.

4.5 Backup Storage

Storage of backups is a serious issue and one that requires careful consideration. Since backups contain critical, and often confidential, company data, precautions must be taken that are appropriate to the type of data being stored. SCoP must establish guidelines for backup storage.

4.6 Backup Retention

When determining the time required for backup retention, SCoP must determine what number of stored copies of backup-up data is sufficient to effectively mitigate risk while preserving required data.

SCoP must have policy in place that defines backup retention periods. The policy must meet industry standards and any applicable legislated requirements.

Backup retention requirements may differ from data retention requirements. SCoP must ensure that policies on data retention are followed. If the policies conflict the greater retention time will apply.

4.7 Restoration Procedures & Documentation

SCoP data restoration procedures must be tested and documented. Documentation must include defined processes with role based accountabilities. Procedures must be clear and concise to prevent misinterpretation by users other than the network (backup) administrator. The procedure documentation must be appended to this policy.

4.8 Restoration Testing

Since a backup policy does no good if the restoration process fails, it is important to periodically test the restore procedures to eliminate potential problems. Backup restores must be tested when any change is made that may affect the backup system, as well as on a regularly scheduled basis.

4.9 Expiration of Backup Media

Certain types of backup media, such as magnetic tapes, have a limited functional lifespan. After a certain time in service the media can no longer be considered dependable. When backup media is put into service the date must be recorded on the media or a master list. The media must then be retired from service after its time in use exceeds manufacturer specifications.

4.10 Applicability of Other Policies

This document will form part of the SCoP cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies must be reviewed as necessary.

5.0 Enforcement

All users are subject to and must comply with this document, SCoP Policy Manual and Code of Conduct, *The Paramedics Act*, *The Health Information Protection Act* (HIPA) and all other applicable legislation and bylaws.

SCoP policies outline corrective and/or disciplinary options for non-compliance. All incidents will be investigated where results and findings could be used as part of disciplinary, contract review or legal actions.

Section IX. Network Access and Authentication

The Saskatchewan College of Paramedics is hereinafter also referred to as "SCoP" or "the College"

1.0 Overview

Consistent standards for network access and authentication are critical to SCoP information security and are often required by regulations or third-party agreements. Any user accessing the SCoP computer systems has the ability to affect the security of all users of the network. An appropriate Network Access and Authentication Policy will reduce risk of a security incident by requiring consistent application of authentication and access standards across the network.

2.0 Purpose

The purpose of this policy is to describe the necessary steps to ensure that users connecting to the corporate network are authenticated in an appropriate manner, in compliance with SCoP standards, and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards.

3.0 Scope

The scope of this policy includes all users who have access to SCoP computers or require access to the corporate network and/or systems. This policy applies not only to employees, but also to guests, contractors, and anyone requiring access to the corporate network. Public access to the SCoP externally-reachable systems (i.e.: SCoP corporate website or public web applications) are specifically excluded from this policy.

4.0 Policies

4.1 Account Setup

Information technology (IT) security starts with strong user security; as such, SCoP requires that potential personnel be screened prior to hire. The level of screening should be appropriate to the position, with more in-depth background checks required for personnel with greater responsibilities or access to confidential information. Examples of acceptable screening methods include checking employment history, criminal records, credit history, and reference checks.

During initial account setup, specific checks must be performed in order to ensure the integrity of the process.

4.2 Account Access Levels

SCoP policy should follow the principle of least privilege, where employees will be provided the least amount of access required to perform their job functions. This is particularly important as it relates to high security zones, such as member investigation files. Any user account with access to these zones (i.e., privileged users) must be given the minimum amount of access possible to perform job functions.

Access levels must be assigned based on job classification or function (role-based access control). SCoP must define the access needs for each role, including systems and data access required to perform job functions as well as the level of privilege required for accessing these resources. Documentation must be kept that details each user's access as well as approval of the user's access privileges by authorized parties.

An access control system that covers all system components must be utilized that enforces this policy, and restricts users' access to data based on defined access levels (based on role/job function). This system must enforce the principle of least access, and have a default "deny all" setting for new or unrecognized users.

4.3 Account Use

All SCoP Network accounts must be managed using a standardized approach that incorporates both legislated and industry standards and requirements. SCoP will ensure that it has policy in place that addresses account use and access to its networks and systems. Account use must be role and/or individual specific and must contain provisions regarding access review.

4.4 Account Termination

When managing network and user accounts, it is important to implement processes that connect human resources decisions with SCoP network administration. This is to ensure that user access is terminated when employment ends or changes.

SCoP must implement a process to notify the appropriate network individual in the event of a staffing change, which includes employment termination or suspension, or a change of job function (promotion, demotion, suspension, etc.) that may require changes in access levels. Access for terminated employees must be immediately revoked.

Additionally, SCoP should develop policy that details regular audit of user accounts that includes the removal or disabling of inactive accounts.

4.5 Network Authentication Requests

User systems must be configured to request authentication against a central network authentication manager, such as a domain, at start-up.

If this authentication mechanism is not available or authentication is unsuccessful, then the user must not be permitted to access the network. SCoP should define re-authentication requirements in order to reactivate sessions that have remained idle for extended periods.

4.6 Database Authentication Requests

SCoP should implement controls to limit access to a database containing confidential data; controls must require authentication, whether the access is by applications, administrators, or users. SCoP must restrict direct database access (i.e.: iMIS) to only database administrators. User access to database information must only occur through queries or programmatic methods (i.e.: stored procedures), rather than direct access.

Database application IDs must only be used by the intended applications, and not individual users or other non-application processes.

4.7 Use of Passwords

When accessing the network, username and password is an acceptable means of authentication. Usernames must be consistent with the requirements set forth in this document, and passwords must conform to the SCoP Password Policy.

4.8 Screensaver Passwords

Screensaver passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason screensaver passwords are required, and must be configured to activate after defined periods (no greater than 30 minutes) of inactivity.

4.9 Minimum Configuration for Access

Any system connecting to the network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in this manner. For this reason, users must strictly adhere to corporate standards with regard to antivirus software and patch levels on their systems.

Users must not be permitted to access the network if these standards are not met. This policy should be enforced with a product that provides network admission control, or through other security controls that forbid access unless explicitly provided.

4.10 Encryption of Login Credentials

Industry best practices state that username and password combinations should never be sent as plain text. If this information were intercepted, it could result in a serious security incident. Therefore, authentication credentials should be encrypted during transmission across any network, whether the transmission occurs internal to the College network or across a public network such as the Internet.

Username and passwords are considered confidential data. When stored, all passwords should be stored in encrypted format (using strong cryptography).

4.11 Failed Login Attempts

Repeated login failures can indicate an attempt to 'crack' a password and inappropriately access a network account. In order to guard against password-guessing and brute-force attempts, SCoP must have policies in place that lock a user's account after a maximum of 3 unsuccessful logins. This can be implemented as a time-based lockout (for a minimum of 30 minutes) or require a manual reset, at the discretion of the Executive Director.

In order to protect against account guessing, when login failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect.

4.12 Alternate Authentication Mechanisms

All policies pertaining to authentication must be viewed as minimum acceptable standards. Where passwords are specified, SCoP has the option to enforce controls that are as secure, or more secure, than passwords, such as tokens or biometrics. When alternate authentication mechanisms are used, the College must ensure that:

- Authentication mechanisms are assigned to an individual account (not shared among multiple users) unless otherwise authorized by the appropriate manager; and,
- Physical and/or logical controls are in place to ensure that only the intended account can use the mechanism to gain access.

Any security incident involving alternate authentication mechanisms must be immediately reported to the Executive Director.

4.13 Applicability of Other Policies

This document will form part of the organization's cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies must be reviewed as necessary.

5.0 Enforcement

All users are subject to and must comply with this document, SCoP Policy Manual and Code of Conduct, *The Paramedics Act*, *The Health Information Protection Act* (HIPA) and all other applicable legislation and bylaws.

SCoP policies outline corrective and/or disciplinary options for non-compliance. All incidents will be investigated where results and findings could be used as part of disciplinary, contract review or legal actions.

Section X: Incident Response Policy

The Saskatchewan College of Paramedics is hereinafter also referred to as "SCoP" or "the College"

1.0 Overview

A security incident can come in many forms including: unauthorized access to the network, infection of systems by virus or other malware, loss of data and/or data integrity, lost or stolen devices containing confidential data, and inappropriate access to data.

This policy is intended to address incidents that may affect the security and integrity of SCoP information assets, more specifically confidential member data, and outlines steps to take in the event of such an incident.

SCoP acknowledges that maintaining effective security is evolutionary and must include regular reassessment of policy and processes in place for both risk assessment and reporting.

2.0 Purpose

This policy is intended to ensure that SCoP is prepared if a security incident were to occur. It details exactly what must occur if an incident is suspected, covering both electronic and physical security incidents. This policy is not intended to provide a substitute for legal advice, and approaches the topic from an information technology (IT) security practices perspective.

3.0 Scope

The scope of this policy covers all physical and information assets owned or provided by the College, whether they reside on the corporate network or elsewhere. External data that interacts with SCoP assets is also subject to this policy. Vendor obligations respecting this policy will be detailed third party contracts or agreements as necessary.

4.0 Policies

4.1 Types of Incidents

A security incident as it relates to this policy and SCoP information assets, may take one of three forms. For the purposes of this policy a security incident may be electronic, physical or a combination of both.

Security incidents can be described as any type of incident verified or suspected, that may have a significant adverse effect on the security of SCoP programs, services, data loss/integrity, and any related function within the organization.

Incidents can include any of the following situations:

- Access to any computer system and/or the SCoP network for any unauthorized purpose;
- Infection by virus outbreak, suspected Trojan or malware;
- Loss of device or print material containing sensitive and/or confidential data;
- Unauthorized/unplanned significant disruption of service; and,
- Unauthorized modifications to SCoP technology or the network.

Also covered in this section are alerts generated from intrusion detection, intrusion prevention, and file integrity monitoring systems.

4.2 Preparation

SCoP will ensure that security controls are in place to prevent or limit damage in the event of an incident. This includes technical tools such as firewalls, intrusion detection systems, authentication, and encryption; and non-technical tools such as physical security for laptops, mobile devices, and printed data.

Additionally, SCoP must ensure that the following is clear to all employees:

- Actions to take when an incident is suspected;
- Incident response roles and responsibilities; and
- Incident notification requirements.

The College will incorporate redundancy where appropriate, to mitigate risk of a catastrophic security incident. Additionally, SCoP must ensure that incident response procedures and policies align with industry and government regulations, and agreements with third parties.

4.3 Confidentiality

All information related to an electronic, physical, or hybrid security incidents must be treated as confidential until the incident is fully contained and investigated. This process will enable the implementation of a deliberate communications approach where appropriate.

For the purpose of this policy, confidential information is defined as: information that if disclosed, could result in increased risk to the organization, its vendors, suppliers, and stakeholders (including members).

4.4 Electronic Incidents/4.5 Physical Incidents/4.6 Hybrid Incidents

When an electronic, physical, or hybrid incident is suspected, the College goal should be to recover as quickly as possible, limit damage (current and future), secure the network, and preserve evidence of the incident.

One of the best ways to prepare for a physical incident is to mandate the use of strong encryption to secure confidential data when stored on College systems, mobile or otherwise. Applicable policies, such as those covering encryption and confidential data, must be reviewed for guidance.

4.5.1 Response

Upon discovering a possible security incident, it is essential that the investigator determine the type of data stored on the missing device. If the type of data cannot be confirmed, and there is a possibility that confidential data was involved, the College must assume that confidential data was lost. SCoP must have policies and procedures in place to manage this type of data loss.

4.5.2 Loss Contained

On confirmation of suspected incident, SCoP will have standards in place to manage incident reporting and management.

4.5.3 Data Loss Suspected

In the event that a data loss is suspected or confirmed, SCoP will have standards in place to manage data loss.

4.7 Notification

In the event that any security incident results in the suspected or confirmed loss of data, SCoP will take the necessary steps to ensure that the College response meets the requirements of applicable legislation and industry standards.

Incident response may also include direct notification to parties, which will be conducted in accordance with SCoP policies and procedures.

The onus is on each and every SCoP user to report an incident once they become aware of a problem. The Executive Director or Deputy Registrar are the first contact point and lead responders in determining the course of action.

For the purpose of this document, an incident is defined as, "Any event that threatens the security of information, assets or personnel." SCoP must have policy in place to manage incident reporting and management.

4.8 Managing Risk

Managing risk of a security incident or data loss is the purpose behind creating and maintaining a comprehensive security policy. Risks can come in many forms: electronic risks like data corruption, computer viruses, hackers, or malicious users; or physical risks such as loss/theft of a device, hardware failure, fire, or a natural disaster. Protecting critical and confidential data and key systems from these risks is of critical importance to the organization.

An Incident Response Policy is not effective at managing risk if it is not maintained and kept current, thus this policy must be reviewed and tested on an annual basis.

4.8.1 Risk Assessment

SCoP must have a defined risk management process in place. Components of the SCoP risk management process must include the implementation of policies and procedures intended to evaluate potential security threats and risks to information in the organization's possession (custody and/or control).

4.8.2 Risk Management Program

The SCoP risk management program must be fully implemented to ensure that risks known to the College are identified through assessment, and that reasonable measures are in place to ensure the continued security of confidential and critical data in the custody and/or control of the organization.

As part of the SCoP risk management program, the Incident Response Policy (IRP) must be reviewed on a regular basis to ensure continued effectiveness and applicability. During this

process, the IRP must be adapted to incorporate changes based on industry or regulatory developments.

4.9 Business Recovery and Continuity Planning

The purpose of recovery and continuity planning is to enable recovery of critical IT systems, operations, and data after an incident by developing coordinated plans, procedures and other technical measures in advance of such a disruptive event.

SCoP must establish and implement policies and procedures for responding to an emergency or other event that damages or negatively impacts access to systems required for business operations, as specified below.

4.9.1 Prioritization

SCoP must identify its critical business resources (and functions), and prioritize them in order to establish a recovery sequence that ensures that the higher-priority resources are recovered before the lower-priority resources. The organization must develop procedures that follow this prioritization and recover each resource based on its criticality.

4.9.2 Develop Recovery Strategies

SCoP must develop recovery strategies to address disruption despite the presence of strong preventative measures. The strategies must identify crucial processes and conditions required for implementation.

The intended outcome of a recovery strategy is to return all SCoP systems to full level of function within an acceptable time frame, within company approved risk parameters (includes risk to reputation, financial, personnel, etc.). Strategies must be certain to take into account, corporate Business Continuity and Business Contingency plans, including system interdependencies and similar linkage with third party vendors. Given that this policy has linkage to the corporate Business Continuity and Contingency plan(s), it is important to ensure that updates to this document are made concurrent with similar updates to these other plans (where available).

The SCoP recovery strategy must reference regularly scheduled data backup and data integrity reviews. These requirements will typically reside within the Business Continuity or Contingency plan(s) and will include standards or off-site storage where required.

SCoP personnel must be aware of their individual (and collective) accountabilities and roles, and must receive training regarding specific responsibilities in the recovery process. The recovery strategies must include procedures for appropriate personnel to access the facility in order to

restore services or lost data. Any necessary vendor contracts required to support the recovery operation must be formalized and put in place prior to an emergency.

4.9.3 Develop Recovery Plan

The recovery plan is perhaps the most important aspect of the Contingency Plan. It must incorporate the recovery strategies developed in the previous section, and organize them into a comprehensive plan.

4.9.3.1 Activation

SCoP must determine under what circumstances the plan will be activated, and define initial steps to be taken. Generally speaking, the recovery plan must be activated when a security incident or emergency occurs or an emergency appears imminent.

4.9.3.2 Assessment

After the plan is activated, SCoP must have assessment processes defined in policy and/or standards.

4.9.3.3 Recovery

The recovery phase must begin as soon as possible after the incident is discovered. Personnel and teams should understand their roles and accountabilities, and be mobilized to activate measures to bring the critical processes and capabilities back online and restore functionality based on a SCoP Business Continuity Plan.

At the end of the recovery phase, all necessary systems must be back online and functioning as needed to support the critical business processes. If the original systems, sites, or facilities are unrecoverable, then operations would have to be fully restored to an alternate site or alternate systems.

4.9.3.4 Appendices

The appendices of the recovery plan should include all the necessary data needed to execute the plan, and may include the following:

- Contact information for team members, managers, and critical vendors;
- Standard Operating Procedures for relevant components;
- Network Diagrams or maps;
- Locations of offsite data, backups, alternate sites, etc.; and,
- Any data that may be necessary to execute the recovery plan

4.9.4 Review, Testing, and Maintenance

As with any critical document, SCoP must develop and implement procedures to review the Business Continuity Plan on a scheduled basis. The review must ensure that the plan is appropriate to restore critical processes after security incidents or critical emergencies.

4.10 Applicability of Other Policies

This document will form part of a SCoP cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies must be reviewed as necessary.

5.0 Enforcement

All users are subject to and must comply with this document, SCoP Policy Manual and Code of Conduct, *The Paramedics Act*, *The Health Information Protection Act* (HIPA) and all other applicable legislation and bylaws.

SCoP policies outline corrective and/or disciplinary options for non-compliance. All incidents will be investigated where results and findings could be used as part of disciplinary, contract review or legal actions.

Section XI: External Connection Policy

The Saskatchewan College of Paramedics is hereinafter also referred to as "SCoP" or "the College"

1.0 Overview

When the need for a SCoP network connection with an external site arises, the connection must be implemented in a secure manner. This can be done by a site-to-site VPN or a direct WAN connection via a telecom/datacom link. Both types of connections are covered by this policy.

A Virtual Private Network, or VPN, provides a method to communicate with remote sites securely over a public medium, such as the Internet. A site-to-site VPN is a dependable and inexpensive substitute for a point-to-point Wide Area Network (WAN). Site-to-site VPNs can be used to connect the LAN to a number of different types of networks: branch or home offices, vendors, partners, customers, etc. As with any external access, these connections need to be carefully controlled through a policy.

Similar to site-to-site VPNs, direct telecom/datacom connections to external entities are sometimes required for business operations. These connections are typically to provide access to vendors or customers for service delivery, or to other business partners. Since SCoP security policies and controls do not necessarily extend to the users of the third parties' networks, these connections can present a significant risk to the network and therefore require careful consideration.

2.0 Purpose

This policy details SCoP standards for site-to-site VPNs and other network connections to external sources. The purpose of this policy is to specify the security standards required for such access, ensuring the integrity of data transmitted and received, and securing the pathways into the network.

3.0 Scope

The scope of this policy covers all connections to sites external to the SCoP network, and covers site-to-site VPNs and direct telecom/WAN connections that are a part of the SCoP infrastructure. This policy also includes both sites requiring access to the SCoP network (inbound) and sites where SCoP connects to external resources (outbound).

4.0 Policies

4.1 Encryption

Site-to-site VPNs must utilize strong encryption to protect data during transmission. Encryption algorithms must meet or exceed current minimum industry standards. Direct connections do not specifically require encryption unless the confidentiality of the data makes encryption necessary.

4.2 Authentication

Site-to-site VPNs must utilize a strong password, pre-shared key, certificate, or other means of authentication to verify the identity of the remote entity. The strongest authentication method available must be used, which can vary from product-to-product.

4.3 Implementation

When site-to-site VPNs or WAN connections are implemented, they must adhere to the principle of least access, providing access limited to only what is required for business purposes.

4.4 Management

SCoP must manage its own VPN gateways; a third party must not provide and manage both sides of the site-to-site VPN, unless this arrangement is covered under an outsourcing agreement. If an existing VPN is to be changed, the changes must only be performed with the approval of the Executive Director.

4.5 Logging and Monitoring

Depending on the nature of the site-to-site VPN or WAN connection, the Executive Director will determine whether additional logging and monitoring is warranted. In general, connections to third parties must be monitored more closely than internal connections.

4.6 Encryption Keys

Site-to-site VPNs are created with pre-shared keys. The security of these keys is critical to the security of the VPN, and by extension, the network. Pre-shared encryption keys must be changed based on SCoP security policy.

If certificates are used instead of pre-shared keys, the certificates must expire and be re-generated after two years.

4.7 Managing Risk

If a VPN or WAN connection is deemed to be a significant security risk, the Executive Director will have the authority to prohibit the connection. If the connection is absolutely required for business functions, additional security measures must be taken at the discretion of the Executive Director.

4.8 Restricting Third Party Access

Best practices for connection to a third party require that the link be held to higher security standards than an intra-company connection. As such, the following standards must be applied:

- Restrict access to the SCoP network to only those users that have a legitimate business need for access.
- Restrict access of those users to only the data and systems they have a business need to access.
- Provide SCoP with other relevant information about individuals that will have access to College data and systems through the connection. SCoP reserves the right to approve or deny this access based on its risk assessment of the connection.
- Provide SCoP with information about individuals that will have access to the SCoP confidential data. The steward or owner of the confidential data will have the right to approve or deny this access for any reason.

4.9 Applicability of Other Policies

This document will form part of the SCoP cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies must be reviewed as necessary.

5.0 Enforcement

All users are subject to and must comply with this document, SCoP Policy Manual and Code of Conduct, *The Paramedics Act*, *The Health Information Protection Act* (HIPA) and all other applicable legislation and bylaws.

SCoP policies outline corrective and/or disciplinary options for non-compliance. All incidents will be investigated where results and findings could be used as part of disciplinary, contract review or legal actions.

Section XII: Wireless Access Policy

The Saskatchewan College of Paramedics is hereinafter also referred to as "SCoP" or "the College"

1.0 Overview

Wireless communication often plays an important role in the workplace. In the past, some type of wireless access was the exception; it has now become the norm in most companies. While wireless access can increase mobility and productivity of users, it can also introduce significant security risks to the network. These risks can be mitigated with a strong Wireless Access Policy.

2.0 Purpose

The purpose of this policy is to state the standards for wireless access to the SCoP network. Wireless access can be provided securely if certain steps are taken to mitigate known risks. This policy outlines the steps that SCoP will take to secure its wireless infrastructure.

3.0 Scope

This policy covers anyone who accesses the network via a wireless connection. The policy further covers the wireless infrastructure of the network, including access points, routers, wireless network interface cards, and anything else capable of transmitting or receiving a wireless signal.

4.0 Policies

4.1 Physical Guidelines

Unless a directional antenna is used, a wireless access point typically broadcasts its signal in all directions. For this reason, access points should be located central to the office space rather than along exterior walls. Technology must be used to control the signal broadcast strength so that it is reduced to only what is necessary to cover the office space. Directional antennas should be used as necessary to focus the signal to areas where it is needed.

Physical security of access points must be considered. Access points must be placed in secured areas of the office. Cabling to and from access points must be secured so that it cannot be easily accessed.

4.2 Configuration and Installation

Wireless environments must change all wireless (vendors) defaults at the point of installation including default wireless encryption keys, passwords and Simple Network Management Protocol (SNMP) community strings. This is of particular importance to wireless environments transmitting confidential data.

4.3 Accessing Confidential Data

When confidential data, is transmitted or accessed via wireless networks, SCoP should use wireless industry best practices for encryption. Only the strongest encryption algorithms must be used to secure this data during transmission. Please note that the use of known insecure encryption methods, such as Wired Equivalent Privacy (WEP), is expressly prohibited.

4.4 Inactivity

Inactive wireless access points must be disabled. If not regularly used and maintained, inactive access points represent an unacceptable risk to the College. This should be accomplished with management software or access point settings if it isn't feasible to do manually.

4.5 Wireless Scans

SCoP must create and document a process to evaluate the network for unauthorized wireless access devices connected to the network, such as wireless access points, wireless cards, and portable wireless devices (such as USB-connectable devices).

4.6 Audits

The wireless network must be audited quarterly to ensure that this policy is being followed.

4.7 Wireless Access Point Inventory

SCoP must document and maintain an inventory of all authorized wireless access points.

4.8 Applicability of Other Policies

This document will form part of the SCoP cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies must be reviewed as necessary.

5.0 Enforcement

All users are subject to and must comply with this document, SCoP Policy Manual and Code of Conduct, *The Paramedics Act*, *The Health Information Protection Act* (HIPA) and all other applicable legislation and bylaws.

SCoP policies outline corrective and/or disciplinary options for non-compliance. All incidents will be investigated where results and findings could be used as part of disciplinary, contract review or legal actions.

Section XIII: Network Security Policy

The Saskatchewan College of Paramedics is hereinafter also referred to as "SCoP" or "the College"

2.0 Purpose

The purpose of this policy is to define minimum acceptable standards and provide guidelines for information technology (IT) security in order to support a secure network infrastructure within SCoP. This section will provide users with practical mechanisms to support a comprehensive set of security policies as laid out in SCoP policies (where applicable).

1.0 Overview

SCoP is committed to providing a secure network infrastructure in order to protect the integrity of corporate data and mitigate risk of a security incident. While security policies typically avoid providing overly-technical guidelines, this policy is by necessity, a more technical document. Where necessary, standards, processes, and requirements are fully detailed for users in individual policy pages that serve as references to sections in this document.

3.0 Scope

This policy covers all information technology (IT) systems and devices that comprise the SCoP network, or that are otherwise controlled by the College.

4.0 Policies

4.1 Network Device Authentication

A compromised password on a network device could have devastating, network-wide consequences. Passwords that are used to secure these devices, such as routers, switches, and servers, must be held to higher standards than user-level or desktop system passwords.

4.1.1 Network Device Password Construction

As passwords are typically user defined they can be a weak link in the corporate security infrastructure. SCoP must have in place, standards that articulate user password requirements.

SCoP recognizes that not every system (internal and external) is compatible with two-factor authentication, or that two-factor authentication is practical in every case. In these situations management must authorize any risk, and identify user requirements regarding password selection.

Where a password must be used, SCoP must mandate that users adhere to defined (minimum) standards regarding password construction. SCoP must also have policy in place regarding authentication of users in system cluster environments.

Password policy must (at minimum) address the following areas:

- Length;
- Syntax;
- Change intervals; and,
- Password re-use.

4.1.2 Failed Logins to Network Devices

Repeated login failures can indicate an unauthorized attempt to access SCoP network accounts. In order to guard against password-guessing and unauthorized access attempts, SCoP must have standards in place limiting the number of invalid login attempts and user account lockout.

In order to protect against account guessing, error messages transmitted to the users should only identify a general error and not identify specifically whether the account name or password were incorrect (i.e.: "the login credentials you supplied were incorrect").

4.1.3 Network Device Default Value Change Requirements

SCoP must have standards in place that define password change requirements. Passwords must be changed as described SCoP Password Policy. Additionally, SCoP must have requirements in place that mandate changes to network device default settings as well as specifications regarding mandatory change requirements where appropriate (i.e.: network compromised).

4.1.4 Password Policy Enforcement

Where passwords are used, SCoP must implement technical controls that enforce College password policies regarding construction, changes, re-use, lockout, etc.

4.1.5 Administrative Password Guidelines

In general, administrative access to systems must be limited to individuals with a legitimate business need for this type of access. SCoP must document the criteria used to validate requirements for system and/or security administration, in addition to capturing processes associated with these functions.

Access must also be evaluated periodically for ongoing business need, and modified accordingly. Where access is removed, SCoP must have processes in place to manage timely response.

4.2 Logging

SCoP must have processes and standards in place to effectively manage ongoing network security. The logging of network access/access attempts should be incorporated into standard operations. Review of logs should also be scheduled and access violations reported based on SCoP processes.

4.2.1 Log Management

While logging is important to SCoP network security, log management can become burdensome without the necessary infrastructure. In order to minimize the time required to review and manage the logs appropriately, SCoP may choose to adopt alternate approaches to support this activity, including log management technology.

4.2.2 Log Review

SCoP should review device logs on a regular basis. Reviews must span all system components and identify anomalies or suspicious activity.

The College must employ legislated and industry standards when conducting a review of access logs. SCoP must ensure that processes are in place to manage the review of critical and high-security access issues in particular. Timing of log reviews will be determined in part, by the organization's overall risk management strategy as well as the discretion of the Executive Director. The frequency of these reviews must be based on the SCoP perceived level of risk.

Exceptions or anomalies discovered during the review process must be fully investigated, and the results documented

4.2.3 Log Retention

Logs must be retained in accordance with the SCoP Log Retention Policy. SCoP must maintain Log retention reports for the greater period, as specified in legislation, policy, and/or standards. The College must classify network device logs as confidential data unless they are known to contain only non-proprietary or public information.

4.3 Audit Trails

Audit trails are similar to logging, and often derived from logs. Where the difference lies is that an audit trail is usually chronological and designed to allow for the reconstruction and examination of the activities surrounding network and system events.

4.3.1 Audit Trail Process

SCoP must ensure that audit processes are in place to monitor individual access to network systems and data. For further clarity audit reports in the context of this compliance document must reflect access to payment card related data and functions. Audit trail records must be retained in a secure environment for a period of no less than 1-year.

4.3.2 What to Record

SCoP must ensure that standards surrounding audit activity are defined in policy and include data elements that must be recorded.

4.3.3 Security of Audit Trails

SCoP must have policy in place that details the standards for audit trail security. The intent of this policy will be to ensure that the integrity of audit logs can be protected.

4.4 Firewalls

A Firewall is a system designed to prevent unauthorized access and/or interaction with a network. Firewall systems can be incorporated using hardware or software components, or both. In the case of a private network, firewalls can be used to monitor traffic moving from the *Internet* to an internal corporate *Intranet* or user computer. The firewall must be able to block messages that fail to meet SCoP network security requirements. Internet connections and other unsecured networks must be separated from the SCoP network through the use of a firewall (i.e.: zones).

4.4.1 Configuration

A process must be developed so that any changes to the firewall configuration must be approved by the Executive Director before being implemented.

4.4.2 Outbound Traffic Filtering

Traffic flowing from the SCoP secure network to a non-secure network has the potential to open the secure area to malicious activity. Firewalls are often configured to block only inbound connections from external sources however, by filtering outbound connections from the network, security can be greatly improved.

SCoP must ensure that firewall configuration takes into consideration the outward flow of traffic and implement solutions to mitigate risks associated with this activity.

4.5 Networking Hardware

Networking hardware, such as routers, switches, bridges, and access points, must be implemented in a consistent manner. SCoP must have standards in place with respect to networking hardware.

4.6 Network Servers

Servers typically accept connections from a number of sources (internal and external) and manage the interactions between these various sources. As a general rule, the more sources that connect to a system, the greater the risk to that system, so it is particularly important to secure network servers. SCoP must have standards in place to ensure the ongoing security of network servers.

4.7 Intrusion Detection/Intrusion Prevention

Intrusion detection and prevention are commonly incorporated into organizational (information technology) security plans to ensure that computers and networks are monitored on a regular basis for unauthorized access. Early alert to unauthorized intrusion can allow system administrators to evaluate potential system or network threats and weaknesses and take remedial action.

Intrusion detection systems (IDS) typically monitor all incoming and outgoing network activity and seek out “suspicious” patterns that may suggest a network or system attack. “IDS” is considered to be a passive-monitoring system, since the main function of an “IDS” is to warn of an unusual activity − not prevent it.

An intrusion prevention system (IPS) provides policies and rules for network traffic, and incorporates intrusion detection processes for alerting network administrators to suspicious activity. This approach allows the administrator to take action upon being alerted (the IPS basically blocks un-approved activity).

SCoP must have policy in place to address intrusion detection and/or intrusion prevention. If IPS is preferred, processes must be defined to guide the system administrator with respect to response. If SCoP selects an intrusion detection system, processes must be defined and implemented to ensure that appropriate levels of monitoring occur and are consistent with those described in SCoP Firewall standards.

4.8 File Integrity Monitoring

File Integrity Monitoring (FIM) will alert system administrators to changes to critical system files. This can be useful to identify potential malicious activity or other significant network events that may otherwise go unnoticed.

SCoP should have processes and standards in place to ensure system file integrity is maintained. Monitoring must take place on a regular basis and may be facilitated through the use of technology. In addition, SCoP must implement processes to respond to any change alerts raised.

4.9 Security Testing

Security testing is an important part of maintaining network security. Security testing may be conducted internally or may be outsourced to a third party provider with no connection to the organization's day-to-day information technology activities.

4.9.1 Wireless Scans

SCoP must have in place, processes to evaluate the network for the presence of all authorized and unauthorized wireless access devices that are connected to the network, such as wireless access points, wireless cards, and portable wireless devices (i.e.: USB-connectable devices).

4.9.2 Internal Vulnerability Scans

SCoP must have policy, processes and/or standards in place to ensure that Internal Vulnerability Scanning is in place to ensure that the College network is evaluated on a regular basis, including following significant changes to the network itself.

4.9.3. External Vulnerability Scans

External Vulnerability Scans, that is, vulnerability scans that test systems from a point external to the network perimeter, must be performed on a scheduled basis. External scans must test the SCoP security posture from a public perspective (the internet). The purpose of these scans is to locate any vulnerability that may exist and can be accessed from external sources.

4.9.4 Penetration Testing

Penetration testing differs from a vulnerability assessment in that penetration testing is a manual process that includes the identification of vulnerabilities present on a network or system, in addition to the active exploit of those vulnerabilities.

The first step in a penetration test is often a vulnerability scan, but a penetration test will then go much deeper, with the intent of simulating a real-world attack and identifying methods an attacker may use to successfully penetrate the network. SCoP should consider implementing testing methodology in place that meets standards as defined in corporate policy.

4.10 Disposal of Information Technology Assets

Information technology assets, such as network servers and routers, often contain sensitive data about the College's network communications. When such assets are decommissioned, SCoP must ensure that policies and procedure are in place to manage this activity.

4.11 Network Compartmentalization

Strong network design is a critical part of ensuring overall network security. Network compartmentalization (separating the network into different segments based on their security classification) allows the organization to reduce its network-wide risk from an attack, virus outbreak, or unauthorized disclosure of confidential information. Firewalls and routers must be configured to seriously restrict or block connections between trusted and untrusted networks. Further, security can be increased if traffic must traverse additional enforcement/inspection points. SCoP should consider developing a policy regarding network compartmentalization.

4.11.1 High Risk Networks and High Security Zones

Examples: Wireless network, member data environment, and systems storing confidential data.

SCoP must have policy and standards in place specific to high risk networks and high security zones that prohibits direct access to and from these areas.

4.11.2 Externally Accessible Networks

Examples: Guest network, email servers, and web servers.

SCoP must have policy and standards in place that segments the external user from the College internal network.

4.11.3 Internal Networks

Examples: SCoP secure drives

SCoP must ensure that standards are in place to protect internal networks from one another thereby also restricting user access to high security areas.

4.12 Network Documentation

Network security documentation is important for efficient and successful network management. The maintenance of "current" documentation ensures that SCoP network administrators have an accurate description of network architecture at any given time.

SCoP should ensure that formal network documentation process and standards are in place.

4.13 Antivirus/Anti-Malware

Computer viruses and malware are significant concerns in today's threat landscape. If a system or network is not properly protected, a virus outbreak can have devastating effects on the system, the network, and the entire company. SCoP must have policy and/or guidelines on the use of antivirus/anti-malware software in place.

4.14 Software Use Policy

Installation of software applications within the corporate technology environment can create significant risk if not managed effectively. SCoP must have policy in place to manage user access and use of software within the Company information technology environment.

4.15 Software/Application Development Policy

This section applies if SCoP develops custom software applications for internal or external use. It is SCoP's intent to develop software in a secure manner and in accordance with industry best

practices for secure application coding. SCoP must have policy in place that address security at all phases of application development.

4.16 Maintenance Windows and Scheduled Downtime

Certain tasks require that network devices be taken offline, either for a simple reboot, an upgrade, or other maintenance. When this occurs, the information technology staff should perform the tasks during a scheduled weekly or monthly maintenance window.

Tasks that are deemed "emergency support," or those that are required to address newly identified vulnerabilities (as determined by the Executive Director), must be done with the SCoP defined notice period to users or immediately if the situation dictates.

4.17 Change Management

Documenting changes to network devices is a good management practice and can help speed resolution in the event of an incident. SCoP must ensure that policies are in place to address network hardware and/or configuration changes. Policy must include standards for change tracking and management including the following:

- Hardware and/or configuration changes to network devices must be documented in a "change log."
- Network devices must employ a method to readily determine device owner and purpose.
- Ports opened to high security zones must be documented (in/outbound)
- Changes to firewall configuration or networking hardware must be documented.

4.18 Suspected Security Incidents

When a security incident is suspected that may impact a network device, SCoP users must refer to the SCoP Incident Response policy for guidance.

4.19 Redundancy

Most organizations consider implementing network redundancy on many levels, from redundancy of individual components to full site-redundancy. As a general rule, the more redundancy implemented, the higher the availability of the device or network, and the higher the associated cost.

Where appropriate, the SCoP Executive Director will determine the appropriate level of redundancy for critical systems and network devices.

4.20 Manufacturer Support Contracts

The use of outdated products can result in a serious security breach. When purchasing critical hardware or software, SCoP must ensure that a maintenance plan, support agreement, or software subscription is in place that will allow the College to receive updates over a specified period of time. The agreement/plan must meet the following minimum requirements:

Hardware: The agreement must contain provisions for the repair/replacement of the device within an acceptable time period, as determined by the Executive Director, as well as provide for software updates on a regular basis.

Software: The arrangement must allow SCoP to access updates, upgrades, and hotfixes for a specified period of time.

4.21 Security Policy Management

In order to ensure that security policy is fully implemented, SCoP will identify security standards and policies (as well as accountabilities necessary) to ensure compliance within the organization. The following sections serve to support this effort.

4.21.1 Information Security Manager

SCoP should designate a specific role within the organization to oversee the corporate security program. The primary function of this role will be to ensure that the College is compliant with this security policy and any other corporate, industry, and/or legislated requirements respecting security – in particular, as related to the payment card industry.

Currently these responsibilities lie with the Executive Director and the SCoP Office Manager. Functions within the purview of these individuals may be delegated, so long as the delegation and accountability are authorized and documented.

4.21.2 Privacy and Security Awareness Training

A security awareness program should be developed that will detail the SCoP information privacy and security program to all users and/or employees covered by the policy, as well as the importance of data security.

The training program must cover, among other topics, the appropriate handling of confidential data, including member personal data. Employees should provide written confirmation on the receipt of, and in agreement to, the user-oriented policies upon hire.

4.21.3 Security Policy Review

The SCoP security policies should be reviewed at least annually. Additionally, the policies must be reviewed when there is an information security incident or a material change to the corporate security policies or network. As part of this evaluation SCoP must review:

- Any applicable regulations for changes that would affect SCoP compliance or the effectiveness of any deployed security controls.
- If SCoP deployed security controls are still capable of performing their intended functions.
- If technology or other changes may have an effect on the SCoP security strategy.
- If any changes need to be made to accommodate future information technology security needs.

4.22 Applicability of Other Policies

This document will form part of the SCoP cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies must be reviewed as necessary.

5.0 Enforcement

All users are subject to and must comply with this document, SCoP Policy Manual and Code of Conduct, *The Paramedics Act*, *The Health Information Protection Act* (HIPA) and all other applicable legislation and bylaws.

SCoP policies outline corrective and/or disciplinary options for non-compliance. All incidents will be investigated where results and findings could be used as part of disciplinary, contract review or legal actions.

Section XIV: Encryption Policy

The Saskatchewan College of Paramedics is hereinafter also referred to as "SCoP" or "the College"

1.0 Overview

Encryption, also known as cryptography, can be used to secure data while it is stored or being transmitted. It is a powerful tool when applied and managed correctly. As the amount of data ScoP must digitally store increases, the use of encryption must be defined and consistently implemented in order to ensure that the security potential of this technology is realized.

2.0 Purpose

The purpose of this policy is to outline ScoP standards for the use of encryption technology so that it is used securely and managed appropriately.

3.0 Scope

This policy covers all data stored on or transmitted across corporate systems.

4.0 Policies

4.1 Applicability of Encryption

Encryption plays a versatile role in ScoP data security. Many policies contain requirements pertaining to encryption including areas such as remote access, mobile devices, emailing and instant messaging back-up, authentication, site to site VPN, confidential data, firewall, and network hardware. Please refer to individual policies covering these respective areas for detailed information.

4.2 Encryption Key Management

Key management is critical to the success of an implementation of encryption technology and must be covered by a set of guidelines related to encryption keys and key management. Management of keys must ensure that data is available for decryption when needed.

4.3 Acceptable Encryption Algorithms

Only the strongest types of generally-accepted, non-proprietary encryption algorithms are allowed, as dictated by industry best practices on encryption. Use of proprietary encryption is specifically forbidden since it has not been subjected to public inspection and its security cannot be assured.

4.4 Legal Use

ScoP must conform to any legislation, regulations, and industry standards for encryption where applicable. Encryption must not be used to hide illegal, immoral, or unethical acts. Individuals doing so will be in violation of this policy and will face immediate consequences as described in the Enforcement section of this document.

4.5 Applicability of Other Policies

This document will form part of the ScoP cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies must be reviewed as necessary.

5.0 Enforcement

All users are subject to and must comply with this document, SCoP Policy Manual and Code of Conduct, *The Paramedics Act*, *The Health Information Protection Act* (HIPA) and all other applicable legislation and bylaws.

SCoP policies outline corrective and/or disciplinary options for non-compliance. All incidents will be investigated where results and findings could be used as part of disciplinary, contract review or legal actions.

Section XV: Outsourcing Policy

The Saskatchewan College of Paramedics is hereinafter also referred to as "SCoP" or "the College"

1.0 Overview

Outsourcing is a logical practice when specialized expertise is required, which happens frequently in many organizations. Trust is necessary for a successful outsourcing relationship, however, the College must be protected by policy that details and enforces the terms of the outsourcing relationship.

2.0 Purpose

The purpose of this policy is to specify actions to take when selecting a provider of outsourced services (including Information Technology), standards for secure communications with the provider, and what contractual terms must be in place to protect the organization.

3.0 Scope

This policy covers any operational requirements and information technology (IT) services being considered for outsourcing.

4.0 Policies

4.1 Deciding to Outsource

Outsourcing services is often necessary but should be carefully considered, since by nature a certain amount of control will be lost by doing so. The following questions must be affirmatively answered before outsourcing is considered:

- Can the service be performed better or less expensively by a third party provider?
- Would it be cost-prohibitive or otherwise unreasonable to perform this service in-house?
- Will outsourcing the service positively affect the quality of this service?
- Is the cost of this service worth the benefit?
- Are any risks associated with outsourcing the service worth the benefit?

4.2 Outsourcing Core Functions

SCoP permits the outsourcing of critical and/or core functions of the corporate Information Technology infrastructure providing outsourcing policies are followed. Examples of these types of functions are data backups, remote access, security, and network management.

SCoP permits the outsourcing of critical and/or core functions of the corporate operational structure providing outsourcing policies are followed. Examples of these types of functions are conducting investigations, research, policy development, and provision of legal advice.

4.3 Evaluating a Provider

Once the decision to outsource a function has been made, selecting the appropriate provider is critical to the success of the endeavor. Due diligence must be performed after the potential providers have been pared to a short list of two to three companies. Due diligence must always be performed prior to a provider being selected.

4.4 Security Controls

In the case of Information Technology outsourcing, the outsourcing contract must provide a mechanism for secure information exchange with the service provider. This will vary with the type of service being outsourced, but may include remote access, VPN, or encrypted file exchange.

SCoP and provider must also maintain a mechanism for verifying the identity of the other party and confirming changes to the service. This will prevent an attacker from using social engineering tactics to gain access to College data.

4.5 Outsourcing Contracts

All outsourced services must be governed by a legal contract, with an original of the executed contract maintained by SCoP.

Contracts must at minimum:

- Cover a specified time period;
- Specify services and associated costing;
- Specify policy for managing confidential information;
- Include a non-disclosure agreement;
- Specify services to be provided, including Service Level Agreements and penalties for missing the targets;

- Allow for cancellation if contractual terms are not met;
- Specify standards for subcontracting of the services and reassignment of contract;
- Cover liability issues; and,
- Describe how and where to handle contractual disputes.

4.6 Access to Information

The provider must be given the least amount of network, system, and/or data access required to perform the contracted services. This access must follow applicable policies and be periodically audited.

4.7 List of Providers

The organization must maintain a list of vendors/service providers with whom confidential data is shared for the purpose of managing secure relationship management. This is part of the ongoing due diligence with respect to outsourced contractors**.**

4.8 Applicability of Other Policies

This document will form part of the College's cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies must be reviewed as necessary.

5.0 Enforcement

All users are subject to and must comply with this document, SCoP Policy Manual and Code of Conduct, *The Paramedics Act, The Health Information Protection Act* (HIPA) and all other applicable legislation and bylaws.

SCoP policies outline corrective and/or disciplinary options for non-compliance. All incidents will be investigated where results and findings could be used as part of disciplinary, contract review or legal actions.

Section XVI: Physical Security Policy

The Saskatchewan College of Paramedics is hereinafter also referred to as "SCoP" or "the College"

1.0 Overview

Information assets are necessarily associated with the physical devices on which they reside. Information is stored on workstations and servers and transmitted on the SCoP physical network infrastructure. In order to secure College data, thought must be given to the security of the physical information technology (IT) resources to ensure that they are protected from standard risks.

2.0 Purpose

The purpose of this policy is to protect SCoP physical information systems by setting standards for secure operations.

3.0 Scope

This policy applies to the physical security of the SCoP information systems, including, but not limited to, all College-owned or College-provided network devices, servers, personal computers, mobile devices, and removable storage media. Additionally, any person working in or visiting the SCoP office is covered by this policy.

Please note that this policy covers the physical security of the SCoP Information Technology infrastructure, and does not cover the security of non-information technology items/areas or employee security. While there will always be overlap, care must be taken to ensure that this policy is consistent with any existing physical security policies.

4.0 Policies

4.1 Choosing a Site

When possible, thought should be given to selecting a site for information technology (IT) operations that is secure and free of unnecessary environmental challenges. This is

especially true when selecting a datacenter or a site for centralized IT operations. At a minimum, the site must meet the following criteria:

- A site should not be particularly susceptible to fire, flood, earthquake, or other natural disasters.
- A site should not be located in an area where the crime rate and/or risk of theft is higher than average.
- A site should have the fewest number of entry points possible.

If these criteria cannot be effectively met for any reason, the College should consider outsourcing its data in whole or in part to a third-party datacenter or hosting provider, provided that such a company can cost effectively meet or exceed the College's requirements.

4.2 Security Zones

At a minimum, SCoP will maintain standard security controls, such as locks on exterior doors and/or an alarm system, to secure the organization's assets. In addition to these controls, SCoP must provide security in layers by designating different security zones within the building that include access by the public and areas deemed private (restricted).

4.3 Access Controls

Access controls are necessary to restrict entry to SCoP premises and security zones to only approved persons. There are several ways to do this, which are outlined in this section.

4.3.1 Keys & Keypads

The use of keys and keypads is acceptable, as long as keys are marked "do not duplicate" and their distribution is limited. These security mechanisms are the most inexpensive and are the most familiar to users.

The disadvantage is that the organization has no control, aside from changing the locks or codes, over how and when the access is used. Keys can be copied and keypad codes can be shared or seen during input. However, used in conjunction with another security strategy, such as an alarm system, strong security can be obtained with keys and keypads.

4.3.2 Keycards & Biometrics

SCoP may require that keycards or biometrics be used for access to security zones designated as private. The organization should consider using these methods for all zones, though it is not required.

Keycards and biometrics have an advantage over keys in that access policies can be defined specific to the individual user (i.e.: access can be limited to forbid off-hours access or specific unauthorized security zones). This approach allows for complete control over exactly who possesses credentials. If a keycard is lost or stolen it can be immediately disabled. If an employee is terminated or resigns, that user's access can be disabled. The granular control offered by keycards and biometrics make them appealing access control methods.

4.3.3 Alarm System

A security alarm system is a good way to minimize risk of theft, or reduce loss in the event of a theft. SCoP should consider developing a policy regarding a monitored alarm system. The system should be monitored 24x7, with SCoP personnel being notified if an alarm is triggered at any time.

4.4 Physical Data Security

SCoP must have policies and procedure in place to ensure that the integrity of the SCoP data is protected. These requirements must at minimum, follow industry standards for data protection when unauthorized access to computers and network equipment occurs.

4.5 Physical System Security

In addition to protecting the data on SCoP information technology assets, specific guidelines are required to secure the systems themselves from physical threat. This policy includes minimum requirements to minimize the risk of loss or theft, damage and tampering. Such policy would include guidelines for training employees to detect and handle tampering.

4.6 Fire Prevention

It is SCoP policy to provide a safe workplace that minimizes the risk of fire. In addition to the danger to employees, even a small fire can be catastrophic to computer systems. Further, due to the electrical components of IT systems, the fire danger in these areas is typically higher than other areas of the College office.

The guidelines below are intended to be specific to the corporate information technology assets and must conform to the SCoP overall fire safety policy.

- Fire, smoke alarms, and/or suppression systems must be used, and must conform to local fire codes and applicable ordinances.
- Electrical outlets must not be overloaded. Users must not chain multiple power strips, extension cords, or surge protectors together.
- Extension cords, surge protectors, power strips, and uninterruptible power supplies must be of the three-wire/three-prong variety.
- Unused electrical equipment must be turned off when not in use for extended periods of time (i.e., during non-business hours) if possible.
- Periodic inspection of electrical equipment must be performed. Power cords, cabling, and other electrical devices must be checked for excessive wear or cracks. If overly-worn equipment is found, the equipment must be replaced or taken out of service immediately depending on the degree of wear.
- A smoke alarm monitoring service must be used that will alert a designated company employee if an alarm is tripped during non-business hours.

4.7 Entry Security

It is the College policy to provide a safe workplace for employees as well as to secure its information assets. Monitoring those who enter and exit the premises is a good security practice in general, but is particularly true for minimizing risk to SCoP systems and data. Guidelines are intended to be specific to SCoP information technology assets and must conform to the SCoP overall security policy, if applicable.

4.8 Applicability of Other Policies

This document will form part of the SCoP cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as necessary.

5.0 Enforcement

All users are subject to and must comply with this document, SCoP Policy Manual and Code of Conduct, *The Paramedics Act, The Health Information Protection Act* (HIPA) and all other applicable legislation and bylaws.

SCoP policies outline corrective and/or disciplinary options for non-compliance. All incidents will be investigated where results and findings could be used as part of disciplinary, contract review or legal actions.