Administrative Policies – Table of Contents

Policy Name	Confidentiality of the Nova Scotia Regulator of Paramedicine Information		
Policy Number:	Administrative – 1.0		
Version Number	2	**Date first Approved:**	09/28/2021
Approved by:	ED/Registrar	**Effective Date:**	09/28/2021
Version Date:	11/15/2024	**Next Review Date:**	

DEFINITIONS

"Board" means the Board of the Regulator;

"Confidential Information" means all confidential, non-public or proprietary information, data, documents, and other materials in whatever form (including, without limitation, in written, oral, visual or electronic form), whether or not such information is marked confidential, that relates to the Regulator, its registrants, employees, Board members, committee and/or working group members, applicants, complainants, respondents, stakeholders, and/or third parties, including, without limitation:

a) personal Information, including personnel records and payroll records;
b) computer system passwords and security codes;
c) research results not yet published, including manuscripts and correspondence;
d) budgetary, service area, or Regulator planning information;
e) information related to litigation that is either pending or in process;
f) all other sensitive information including intellectual research findings, intellectual property, and financial data;

"Employee" means any individual employed by the Regulator, whether on a permanent, temporary, or part-time basis;

"Personal Information" has the meaning ascribed to it in the Regulator's "Privacy Policy";

"Privacy Breach" has the meaning ascribed to it in the Regulator's "Responding to a Breach of Privacy Policy";

"Regulator" means the Nova Scotia Regulator of Paramedicine;

"Third-Party Service Provider" means any individual or entity that provides services to the Regulator and is not employed by the Regulator; and

"Volunteer" means any individual who volunteers with the Regulator, including, without limitation, any member of the Board, or any member of any committee or working group of the Regulator, including those who may receive renumeration and/or honoraria from the Regulator.

POLICY STATEMENT

1. This policy applies to all:

   (a) Employees;
   (b) Volunteers;
   (c) Third-Party Service Providers; and
   (d) Confidential Information.

2. The Regulator shall adhere to its obligations related to its handling and protection of Confidential Information, and shall ensure Employees, Board members, Volunteers, and Third-Party Service Providers of the Regulator are knowledgeable and fully informed of their obligations respecting Confidential Information.

3. The Regulator protects and safeguards Confidential Information entrusted to it by Employees, Volunteers, registrants, applicants, stakeholders and other third parties from unauthorized access, use, and disclosure.

4. All Employees and Volunteers shall sign a confidentiality agreement with the Regulator.

5. At all times throughout and following a term of employment or term of office, Employees and Volunteers have a duty to keep confidential and protect against unauthorized use or disclosure all Confidential Information, in accordance with the confidentiality agreement.

6. All Third-Party Service Providers with access to Confidential Information shall sign an agreement prior to being given access to such information.

7. At all times during and following a Third-Party Service Provider's engagement with the Regulator, all Third-Party Service Providers have a duty to keep confidential and protect against unauthorized use or disclosure all Confidential Information, in accordance with the agreement.

8. Confidential Information shall be kept in safe and secure locations and shall not be accessible to the public.

9. Computerized records with limited user access and computer terminals shall not be accessible to anyone other than users authorized by the Regulator.

10. All Personal Information shall be collected, used, accessed, stored, and disclosed in only in accordance with the Regulator's "Privacy Policy", and any Privacy Breach shall be handled in accordance with the Regulator's "Responding to a Breach of Privacy Policy".

11. If an individual or entity has not given their signed consent for the Regulator to disclose their Confidential Information to another source, such consent will be sought, or the information will not be divulged unless the Regulator is legally authorized or required to do so.

12. Unauthorized use and disclosure of Confidential Information may lead to disciplinary action, up to and including immediate termination of employment or appointment, legal action, and/or termination of any agreements or contracts with the Regulator.

13. To ensure protection of the Regulator's Confidential Information, and Confidential Information in its custody or control, the Privacy Officer is responsible for managing all inquiries from any third party, including, without limitation, the press, and/or media, regarding the Regulator or Confidential Information.

14. All third-party inquiries requesting Confidential Information shall be immediately referred to the Privacy Officer.

RELATED DOCUMENTS

Policy Adm 1.0 – Confidentiality of Nova Scotia Regulator of Paramedicine Information
Attachment A – Confidentiality Agreement

DOCUMENT HISTORY ((Date of Reviews. Revisions, etc):

Attachment "A"

Confidentiality Agreement

This Confidentiality Agreement is entered into, by the signatory, on the below date. This agreement applies to all:

a) Employees;
b) Volunteers;
c) Third-Party Service Providers; and
d) Confidential Information.

In this agreement, "Confidential Information" means all confidential, non-public or proprietary information, data, documents, and other materials in whatever form (including, without limitation, in written, oral, visual or electronic form), whether or not such information is marked confidential, that relates to the Regulator, its registrants, employees, Board members, committee and/or working group members, applicants, complainants, respondents, stakeholders, and/or third parties, including, without limitation:

a) personal Information, including personnel records and payroll records;
b) computer system passwords and security codes;
c) research results not yet published including manuscripts and correspondence;
d) budgetary, service area, or Regulator planning information;
e) information related to litigation that is either pending or in process;
f) all other sensitive information including intellectual research findings, intellectual property, and financial data;

"Personal Information" means any information about an identifiable individual or information that, when combined with other information, whether readily available or not, may identify or tend to identify an individual, as may be defined or limited under applicable privacy legislation. Personal Information does not include anonymous or de-identified data that is not associated with a particular individual.

I have read and have been provided with the opportunity to obtain additional information regarding the following Administrative Policies of the Regulator:

- 1.0 Confidentiality of Nova Scotia Regulator of Paramedicine Information
- 1.1 Privacy Policy
- 1.2 Collection and Use of Employee Personal Information
- 1.3 Responding to a Privacy Breach

I understand that as a signatory to this agreement I:

- have a duty to handle and protect Confidential Information in my possession and control;
- am knowledgeable and fully informed of my obligation respecting to Confidential Information in my possession and control;

- must keep confidential and protect against unauthorized use or disclosure of Confidential Information;
- will keep Confidential Information in a safe and secure place and shall ensure it is not accessible to the public;
- shall not allow unauthorized access to computerized records with limited user access and/or computer terminals, or other electronic devices;
- shall only collect, use, access, store and disclose Personal Information in accordance with the Regulator's "Privacy Policy" and that any privacy breach shall be handled in accordance with the Regulator's "Responding to a Breach of Privacy Policy";
- must seek consent from an individual or entity who has not provided their signed consent for the Regulator to disclose their Confidential Information to another source, otherwise the information will not be divulged unless the Regulator is legally authorized or required to do so;
- understand that unauthorized use and disclosure of Confidential Information may lead to disciplinary action, including immediate termination of employment or appointment, legal action, and/or termination of any agreements or contracts with the Regulator; and
- understand the Privacy Officer is responsible for managing all inquiries from any third-party, including, without limitation, the press, and/or media, regarding the Regulator or Confidential Information and will refer all such inquiries to the Privacy Officer.

I acknowledge that any violation of this agreement could cause harm to the Regulator and frustrate the Regulator's work. Therefore, as a signatory to this agreement I recognize that unauthorized use and disclosure of Confidential Information my lead to disciplinary action, including immediate termination of employment or appointment, legal action, and/or termination of any agreements or contracts with the Regulator.

I will direct any questions regarding my confidentiality obligations to the Executive Director/Registrar of the Regulator. I have read and understand the above expectations within this agreement and more broadly within the Confidentiality and Privacy Policies of the Regulator and agree to abide by this duty of confidentiality.

Signatory:

_____

Print Name

_____ _____

Signature *Date*

Regulator Staff:

_____

Print Name

_____ _____

Signature *Date*

Policy Name:	Privacy		
Policy Number:	Administrative – 1.1		
Version Number:	1	**Date first Approved:**	09/28/2021
Approved by:	ED/Registrar	**Effective Date:**	09/28/2021
Version Date:	11/15/2024	**Next Review Date:**	

DEFINITIONS

"Act" means the *Regulated Health Professions Act*, SNS 2023, c 15;

"CSA Model Code" means the Canadian Standards Association Model Code for the Protection of Personal Information;

"Personal Information" means any information about an identifiable individual or information that, when combined with other information, whether readily available or not, may identify or tend to identify an individual, as may be defined or limited under applicable privacy legislation. Personal Information does not include anonymous or de-identified data that is not associated with a particular individual; and

"Privacy Officer" means the Executive Director/Registrar of the Regulator, or their designate.

"Regulations" means the Regulated Health Professions General Regulations and the Paramedicine Regulations;

"Regulator" means the Nova Scotia Regulator of Paramedicine;

POLICY STATEMENT

1. The Regulator is committed to protecting the privacy and security of the Personal Information and is accountable for all Personal Information under its control.

2. The Regulator will adhere to the CSA Model Code with respect to all Personal Information within its care and control relating to registrants of and applicants to the Regulator, as well as complainants and third parties who provide Personal Information to the Regulator.

3. This policy does not apply to employees of the Regulator.

Accountability

4. The Regulator is accountable for all Personal Information under its control.

5. The Regulator collects, uses, and discloses Personal Information in accordance with its obligations under the Act, the Regulations, the CSA Model Code, and all applicable privacy legislation.

6. The Regulator has designated a Privacy Officer, who is responsible for everyday operation and control of Personal Information and the Regulator's compliance with this policy.

7. From time to time, the Regulator discloses Personal Information to third parties for administrative and licensing purposes.

8. Third parties are required to sign confidentiality agreements which reinforce the strict confidentiality obligations on them.

Identifying Purposes

9. The Regulator is required, pursuant to the *Act*, to regulate the practice of paramedicine in the province of Nova Scotia in the public interest, and the Regulator collects and uses Personal Information to carry its public interest mandate and as permitted or required under applicable legislation.

10. The types of information, including Personal Information, the Regulator may collect from its registrants and applicants include:

    a) names, addresses, telephone numbers, email addresses, and/or other contact information;
    b) date of birth, social insurance number, gender, age, marital status, nationality;
    c) educational information, such as educational program name and graduation year, proof of program completion, proof of entry to practice exam completion;
    d) past licensure status;
    e) past and current employment information;
    f) language proficiency;
    g) opinions about or decisions regarding the registrant or applicant, including
        i. academic and/or professional references, clinical and competence assessments, mental health and physical health assessments, professional conduct, practice review, fitness to practise, registration/licensing and/or reinstatement decisions of the Regulator, and decisions from other regulatory bodies; and
        ii. criminal record checks and vulnerable sector checks.

11. In the event of a complaint, the Regulator may collect Personal Information from or about the complainant, including:

    a) names, addresses, telephone numbers, email addresses, or other contact information; and
    b) Personal Health Information, as defined in the *Personal Health Information Act*, SNS 2010, c 41.

12. The purposes for which the Regulator collects and uses Personal Information includes, but is not limited to:

a) registration and licensing applications and renewals;
b) credentials verification and assessment, which may include sharing of Personal Information with other regulatory bodies in Canada;
c) recording registrant status and establishing and maintaining updated Register listings to publish on the Regulator website and made available to inquirers;
d) complaints and investigations;
e) communication with registrants and applicants;
f) regulatory processes;
g) publication distribution;
h) compilation of statistics;
i) payment of the annual licensing fee; and
j) surveys.

Consent

13. The Regulator is dedicated to ensuring that registrants, applicants, complainants and other third parties are aware of the purposes for which Personal Information is collected, the reasons for the use of the information, and reasons for disclosure.

14. Where required, the Regulator obtains consent from individuals for the collection, use and disclosure of Personal Information.

15. In certain circumstances, the consent of the individual can be obtained after collection of the information, but before its use.

16. The Regulator will not, as a condition of the supply of goods or services, require that an individual consent to the collection, use, or disclosure of information beyond what is required for legitimate and communicated purposes.

17. Some information related to registration and licensing, competence and professional development must be provided as a condition of obtaining and maintaining registration and licensing.

18. There may be circumstances where consent may be implied, and in such cases, the purpose for the collection and use of Personal Information must be apparent and the Regulator may only use the Personal Information for the apparent purpose, and the Regulator will not use that information for any other purpose.

19. The Regulator may collect and use Personal Information in circumstances where the collection and/or use of such information is clearly in the interests of the individual and consent cannot be obtained in a timely manner.

20. Similarly, Personal Information may be collected and used without the consent of the individual if the information is reasonably required to investigate a breach of an agreement, a violation of the law, or investigations related to professional conduct,

conduct unbecoming, incompetence, and/or incapacity and there is reason to believe that obtaining consent may compromise the availability or accuracy of such information.

21. Individuals can withdraw consent at any time for the retention and use of Personal Information, but only to the extent that such consent withdrawal does not affect the ability of the Regulator to carry out its statutory functions or comply with its obligations under law, and the Regulator will inform the individual of the implications of such withdrawal.

Limiting Collection

22. The Regulator collects Personal Information only to the extent necessary for the purposes identified, and Personal Information is collected in a fair and lawful manner.

Limiting Use, Disclosure and Retention

23. The Regulator does not sell or trade Personal Information to third parties.

24. Personal Information is only used or disclosed by the Regulator for the purpose for which it was collected, unless otherwise authorized or required by law.

25. The Regulator discloses Personal Information to the following third parties for the following purposes:

    a) Nova Scotia Department of Health and Wellness for use in the electronic health record "Provider Registry" and paramedic and EMR human resources planning; and
    b) Canadian Institute of Health Information (CIHI) for statistical health reporting.

26. In accordance with its statutory obligations, the names of the Regulator's registrants, their registration number, their practising status, as well as any registration and/or licensing conditions, restrictions and/or sanctions applicable to the registrant, may be made available to employers, other regulators, and the public, including by posting on the Regulator's website.

27. Except as otherwise permitted or required by applicable legislation, the Regulator will only retain Personal Information for as long as necessary to fulfil the purposes for which it was collected, including for the purposes of satisfying any legal, accounting, or reporting requirements.

Accuracy

28. The Regulator is dedicated to maintaining the Personal Information under its control in a form that is accurate, complete, and current as is necessary for the fulfilment of the Regulator's purposes.

29. Individuals are encouraged to contact the Regulator and update any changes to their Personal Information.

Safeguards

30. The Regulator takes reasonable steps to ensure that Personal Information is protected against loss, unauthorized access, use, disclosure, and alteration, and this protection applies to both electronic and hard copy forms of Personal Information.

31. The safeguards used by the Regulator to protect Personal Information include:

    a) technological measures, such as the use of passwords and data encryption for electronic information;
    b) physical measures, such as locked filing cabinets and restricted access to areas where Personal Information is stored;
    c) organizational measures, such as employee training, confidentiality agreements, and limited access on a "need to know" basis;
    d) third-party measures, such as confidentiality agreements with third parties; and
    e) destruction measures, such as on-site shredding and physical destruction of hard drives.

Openness

32. The Regulator is open about its policies and procedures and will provide individuals with specific information relating to the maintenance of Personal Information, and these policies are available by contacting the Regulator's Privacy Officer.

Individual Access

33. Individuals may contact the Privacy Officer at any time to discuss access to their Personal Information in the possession of the Regulator, and upon written request, access may be provided, and a fee may be applied to cover the cost of administration.

34. In certain situations, such as legal or regulatory requirements, the Regulator may not be able to offer the individual access to their Personal Information and, in such cases, the Regulator will provide the individual with the reasons for denial.

35. The Regulator will correct or amend Personal Information that is shown to be incomplete or inaccurate.

Challenging Compliance

36. The Privacy Officer is responsible for overseeing compliance with this Privacy Policy.

37. Any questions about compliance with this Privacy Policy can be directed to the Privacy Officer who will respond to any concerns.

38. The Regulator may investigate a complaint and may take appropriate action to resolve the issue.

RELATED DOCUMENTS

Policy Adm 1.0 – Confidentiality of Nova Scotia Regulator of Paramedicine Information
Attachment A – Confidentiality Agreement

DOCUMENT HISTORY (Date of Reviews. Revisions, etc):

Policy Name	Collection and Use of Employee Personal Information		
Policy Number:	Administrative – 1.2		
Version Number:	1	**Date first Approved:**	09/28/2021
Approved by:	ED/Registrar	**Effective Date:**	09/28/2021
Version Date:	11/15/2024	**Next Review Date:**	

DEFINITIONS

"Board" means the Board of the Regulator;

"Employee" has the meaning ascribed to it in the Regulator's "Confidentiality of NSRP Information Policy";

"Personal Information" means any information about an identifiable individual or information that, when combined with other information, whether readily available or not, may identify or tend to identify an individual, as may be defined or limited under applicable privacy legislation. Personal Information does not include: (i) an Employee's business contact details and job title; or (ii) anonymous or de-identified data that is not associated with a particular individual;

"Privacy Officer" means the Executive Director/Registrar of the Regulator, or their designate;

"Regulator" means the Nova Scotia Regulator of Paramedicine;

"Third-Party Service Provider" has the meaning ascribed to it in the Regulator's "Confidentiality of Nova Scotia Regulator of Paramedicine Information Policy"; and

"Volunteer" has the meaning ascribed to it in the Regulator's "Confidentiality of Nova Scotia Regulator of Paramedicine Information Policy".

POLICY STATEMENT

1. The Regulator is committed to protecting the privacy and security of Employee Personal Information.

2. This Policy describes the categories of Personal Information that the Regulator collects, how the Regulator uses the Personal Information, how the Regulator secures Personal Information, when the Regulator may disclose Personal Information to third parties, and when the Regulator may transfer Personal Information inside or outside of Canada.

3. The Regulator will only use the Personal Information of its Employees in accordance with this Policy, unless otherwise authorized or required by law.

4. The Regulator will take steps to ensure that the Personal Information that it collects is adequate, relevant, not excessive, and used for limited purposes.

5. This policy applies to current and former Employees of the Regulator.

6. To carry out its activities and obligations as an employer, the Regulator may collect, store, and use the following categories of Personal Information, which it requires to administer the employment relationship with its Employees:

    a) personal contact details such as name, title, addresses, telephone numbers, personal email addresses;
    b) date of birth;
    c) sex;
    d) gender;
    e) marital and dependent status;
    f) beneficiary and emergency contact information;
    g) government identification numbers such as social insurance or other national insurance number, driver's license number, or other identification card number;
    h) bank account details and payroll information;
    i) wage and benefit information;
    j) compensation history, including:
        i) performance information;
        ii) insurance enrolment information;
        iii) start date;
        iv) employment location;
        v) education and training;
        vi) employment records (including professional memberships, references, work history, and proof of eligibility for employment;
        vii) photograph; and
        viii) other personal details that may be included in a resume or cover letter.

Use of Personal Information

7. The Regulator will only use Personal Information where applicable law permits or requires it, for example, when necessary for the performance of the employment contract with the Employee, or when the use is necessary to comply with a legal obligation that applies to the Regulator.

8. The Regulator may use Personal Information for the following legitimate business purposes:

    a) employee administration (including payroll and benefits administration);
    b) business management and planning;

    c) processing Employee work-related claims (for example, insurance and worker's compensation claims);
    d) accounting and auditing;
    e) conducting performance reviews and determining performance requirements;

f) assessing qualifications for a particular job or task;
g) gathering evidence for disciplinary action or termination of employment;
h) complying with applicable law;
i) education, training, and development requirements;
j) health administration services; and
k) complying with health and safety obligations.

9. The Regulator will only use Personal Information for the purposes for which it was collected.

10. If the Regulator needs to use Personal Information for an unrelated purpose, the Regulator will notify the Employee and, if required by law, seek the Employee's consent.

11. The Regulator may use Personal Information without Employees' knowledge or consent where authorized or required by applicable law or regulation.

Disclosure of Personal Information

12. The Regulator will only disclose Personal Information to third parties where authorized or required by law or to the Regulator's Employees, Volunteers and Third-Party Service Providers who require it to assist the Regulator with administering the employment relationship with the Employee, including Third-Party Service Providers who provide services to the Regulator or on the Regulator's behalf.

13. The Regulator requires all its Third-Party Service Providers to implement appropriate security measures to protect Personal Information consistent with the Regulator's policies and any data security obligations applicable to the Regulator.

14. The Regulator permits its Third-Party Service Providers to use Personal Information only for specified purposes in accordance with the Regulator's instructions, and not for their own purposes.

15. The Regulator may further disclose Personal Information for the following additional purposes where permitted or required by applicable law:

a) to comply with legal obligations or valid legal processes such as search warrants, subpoenas, or court orders;
    i) to comply with a legal obligation or legal process, the Regulator will take reasonable steps to ensure that only the minimum Personal Information necessary for the specific purpose and circumstances is disclosed;
b) during emergency situations or where necessary to protect the safety of persons;
c) where the Personal Information is publicly available; and
d) for additional purposes with Employee consent where such consent is required by law.

Security

16. The Regulator has implemented appropriate physical, technical, and organizational security measures designed to secure Personal Information against accidental loss and unauthorized access, use, alteration, or disclosure.

    a) All Employee Personal Information is maintained in electronic form, safeguarded using password protection, and secured within the Regulator's Microsoft 365 One-drive system;
    b) any paper documents completed by Employees containing Personal Information shall be scanned and maintained in accordance with the foregoing, and the paper documents shall then be destroyed by shredding; and
    c) the Regulator limits Personal Information access to those Employees, Volunteers and Third-Party Service Providers, and other third parties that have a legitimate business need for such access.

Retention

17. Except as otherwise permitted or required by applicable law or regulation, the Regulator will only retain Personal Information for as long as necessary to fulfil the purposes for which it was collected, including for the purposes of satisfying any legal, accounting, or reporting requirements.

18. Under some circumstances the Regulator may anonymize Personal Information so that it cannot be associated with the Employee.

19. The Regulator reserves the right to use such anonymous and de-identified data for any legitimate business purpose without further notice to the Employee and without their consent.

20. Once an individual is no longer an Employee of the Regulator, the Regulator will retain and securely destroy the Employee's Personal Information in accordance with applicable laws and regulations.

Rights of Access, Correction, Erasure, and Objection

21. Employees must ensure that their Personal Information held by the Regulator is accurate and current.

22. Employees have the right to request access to and to correct their Personal Information held by the Regulator, or to withdraw their consent to the use of their Personal Information under certain circumstances.

23. If an Employee seeks to review, verify, correct, or withdraw consent to the use of their Personal Information, they shall contact the Privacy Officer, and any such communication shall be in writing.

24. The Regulator may request specific information from an Employee to help confirm the Employee's identity and their right to access, and to provide the Employee with their Personal Information held by the Regulator or make requested changes.

25. Applicable law may allow or require the Regulator to refuse to provide the Employee with access to some or all the Personal Information held about them, or the Regulator may have destroyed, erased, or made Personal Information anonymous in accordance with its record retention obligations and practices.

26. If the Regulator cannot provide the Employee with access to their Personal Information, the Regulator will inform the Employee of the reasons why, subject to any legal or regulatory restrictions.

Privacy Officer

27. The Privacy Officer is responsible for overseeing compliance with this Policy, and any enquiries related to this Policy or how Personal Information is handled shall be directed to the Privacy Officer.

RELATED DOCUMENTS

Policy Adm 1.0 – Confidentiality of Nova Scotia Regulator of Paramedicine Information
Attachment A – Confidentiality Agreement

DOCUMENT HISTORY (Date of Reviews, revisions, etc):

Policy Name	Responding to a Breach of Privacy		
Policy Number:	Administrative – 1.3		
Version Number	1	**Date first Approved:**	09/28/2021
Approved by:	ED/Registrar	**Effective Date:**	09/28/2021
Version Date:	11/15/2024	**Next Review Date:**	

DEFINITIONS

"Board" means the Board of the Regulator;

"Employee" has the meaning ascribed to it in the Regulator's "Confidentiality of Nova Scotia Regulator of Paramedicine Information Policy";

"Personal Information" has the meaning ascribed to it in the Regulator's "Privacy Policy";

"Privacy Breach" means any occurrence where there is confirmed inappropriate or unauthorized access to or collection, use, disclosure, or disposal of Personal Information, in contravention of applicable privacy legislation or the Regulator's policies/procedures;

"Privacy Officer" means the Executive Director/Registrar of the Regulator, or their designate;

"Regulator" means the Nova Scotia Regulator of Paramedicine;

"Third-Party Service Provider" has the meaning ascribed to it in the Regulator's "Confidentiality of Nova Scotia Regulator or Paramedicine Information Policy"; and

"Volunteer" has the meaning ascribed to it in the Regulator's "Confidentiality of Nova Scotia Regulator of Paramedicine Information Policy".

POLICY STATEMENT

1. Employees, Volunteers and Third-Party Service Providers of the Regulator are required to:

    a) be knowledgeable of the procedures in place to prevent and manage Privacy Breaches;
    b) ensure the Regulator complies with all applicable privacy laws governing Personal Information in its custody or control;
    c) demonstrate to stakeholders that a systematic procedure is in place to respond to and deal with a Privacy Breach;
    d) encourage prompt identification, reporting, and resolution of Privacy Breaches.

2. This policy applies to all:

    a) Employees;
    b) Volunteers; and

c) Personal Information in the custody or control of the Regulator.

PROCEDURE

3. The procedures below describe the approach the Regulator will employ for managing an actual or suspected Privacy Breach.

4. While the general order of events required to take place is as outlined below, tasks may occur in very quick succession or simultaneously.

Identification, Reporting and Documentation

5. The person who identifies an actual or suspected Privacy Breach shall immediately notify the Privacy Officer, and the Privacy Officer will work with the individual who identified the Privacy Breach to document the Privacy Breach on the Privacy Breach Checklist attached as Attachment A.

Containment

6. The person who identified the actual or suspected Privacy Breach shall, in consultation with the Privacy Officer, take immediate and common-sense actions to contain the Privacy Breach by, for example:

a) stopping the unauthorized practice;
b) shutting down the system that was breached;
c) recovering the Personal Information and all copies, ensuring no copies of Personal
d) Information have been made or retained by any unauthorized person;
e) revoking or changing computer access codes;
f) sending a remote "kill" signal to a lost or stolen portable storage device;
g) correcting weaknesses in physical security; and
h) notifying the police if a Privacy Breach appears to involve theft or other criminal activity.

7. The Privacy Officer shall promptly ensure that all steps that are required to contain the Privacy Breach are taken, including any of the steps enumerated above.

8. The Privacy Officer, along with the person who identified the actual or suspected Privacy Breach, shall take all necessary actions to preserve any evidence associated with the Privacy Breach, including by being careful not to destroy evidence that may be valuable in determining the cause of the Privacy Breach or will allow the Regulator to take appropriate corrective action.

Investigation and Risk Assessment

9. The Privacy Officer will investigate to understand and document the circumstances associated with the Privacy Breach and determine:

    a) what happened, when the Privacy Breach occurred (if known), who discovered it, when it was discovered, and how it was discovered;
    b) the nature and sensitivity of the Personal Information involved;
    c) the apparent cause of the Privacy Breach;
    d) the relationship between the recipient(s) of the information and the individual(s) affected by the Privacy Breach;
    e) the scope and extent of the Privacy Breach e.g., number of individuals affected, number of records involved, system(s) breached, the number of likely recipients of the Personal Information, the risk of further access, use or disclosure, including in mass media or online; and
    f) the effectiveness of the containment efforts.

10. To understand the facts, the investigation may include steps such as:

    a) interviewing individuals involved with the Privacy Breach or individuals who can provide information about the process and confirm details;
    b) obtaining and reviewing relevant documentation;
    c) observing, visiting, or inspecting the site of the Privacy Breach; and
    d) consulting with external resources, such as legal advisors, security experts, and/or law enforcement officials, where and when appropriate.

11. The Privacy Officer shall analyse the cause(s) and extent of the Privacy Breach to identify:

    a) system-induced causes (e.g., technical error, system compromise);
    b) human causes (e.g., human error; theft; unauthorized access; loss);
    c) whether the Privacy Breach can be attributed to a systemic (organizational) issue, gap, or risk or to an isolated incident; and
    d) whether there is there a risk of ongoing or further exposure of the information.

12. Considering the circumstances, facts and cause(s) of the Privacy Breach, the Privacy Officer shall conduct a risk assessment, including whether the Privacy Breach poses a real risk of significant harm to the affected individual(s).

Assessment and/or Notification

13. The Privacy Officer shall review the risk assessment and consider the circumstances and facts of the Privacy Breach to determine whether individual(s) affected by the Privacy Breach should be notified. In making this determination, the Privacy Officer shall consider:

a) whether there are any statutory, regulatory, or contractual notification requirements governing the Regulator or which apply in connection with the Privacy Breach;
b) whether there is a risk of identity theft or fraud;
c) whether there is a risk of physical harm;
d) whether there is a risk of hurt, humiliation, or damage to reputation;
e) whether there is a risk of loss of business or employment opportunities; and
f) whether a risk of loss of confidence in the Regulator's ability to regulate the profession dictates that notification is appropriate.

14. If the Privacy Officer determines that individuals affected by the Privacy Breach should be notified, the Privacy Officer shall notify the affected individual(s) as soon as practicable, and such notification shall be provided directly, either by phone, letter, email, or in person, unless it is unreasonable or inappropriate to do so.

15. To the extent practicable, the notification shall include the following information:

a) date of the Privacy Breach;
b) description of the Privacy Breach;
c) description of the Personal Information inappropriately accessed, collected, used, or disclosed;
d) risk(s) to the individual caused by the Privacy Breach, if any;
e) the steps taken to date to control or reduce the harm;
f) further steps planned to prevent future Privacy Breaches;
g) steps the individual can take to further mitigate the risk of harm; and
h) contact information of the Privacy Officer who can answer questions or provide any further information.

16. The Privacy Officer shall review the risk assessment and consider the circumstances and facts of the Privacy Breach to determine whether any other authorities or organizations should be notified including the police, insurers, professional regulatory bodies, or other internal or external parties not already notified.

Prevention

17. The Privacy Officer shall consider the results of the investigation and the cause of the Privacy Breach for the purpose developing or improving preventative measures and safeguards to reduce the impact and likelihood of future Privacy Breaches.

18. Preventative measures may include, for example:

a) an audit of and improvements to physical safeguards (e.g. access to filing cabinets, office security, computer security);
b) an audit of and improvements to technical safeguards (e.g. encryption, password protection);

c) a review of training practices and recommendations to change or enhance training on specific topics;
d) a review of policies and procedures and recommended revisions to reflect the lessons learned;
e) a review of existing processes to determine if improvements are required;
f) education of the Employees, Volunteers and Third-Party Service Providers of the Regulator on how to avoid similar breaches; and
g) requiring individual(s) involved in the Privacy Breach to take additional privacy training to enhance the individuals' understanding of this Policy, the Regulator's privacy obligations, and how to reduce the risk of future Privacy Breaches.

Accountability

19. The Privacy Officer shall:

a) monitor and promote compliance with this policy;
b) review this policy at a minimum every three years to determine its effectiveness and recommend amendments if needed;
c) maintain procedures to support an effective response to any Privacy Breach;
d) ensure Privacy Breaches, related investigations, and resolutions are properly documented;
e) ensure Privacy Breaches are reported to the Regulator's stakeholders when required in the circumstances, in a timely manner;
f) work collaboratively with stakeholders to resolve Privacy Breaches in a manner that minimizes risks to the Regulator, its stakeholders, and impacted individuals; and
g) identify preventative measures and monitor their completion.

20. Employees, Volunteers, and Third-Party Service Providers of the Regulator who handle Personal Information when carrying out their duties on behalf of the Regulator are required to:

a) know, understand, and comply with their obligations under this policy; and
b) immediately report any actual or suspected Privacy Breaches or privacy complaints to the Privacy Officer.

RELATED DOCUMENTS

Policy Adm 1.0 – Confidentiality of Nova Scotia Regulator of Paramedicine Information, Attachment A – Confidentiality Agreement
Policy Adm 1.3 - Responding to a Breach of Privacy, Attachment A - Privacy Breach Checklist

DOCUMENT HISTORY (Date of Reviews, Revisions, etc):

Attachment "A"

Privacy Breach Checklist

This checklist will be utilized to evaluate the Nova Scotia Regulator of Paramedicine's response to a Privacy Breach.

Date of report: _____

Date breach initially discovered: _____

Contact information: _____

Contact Person (Report Author): _____

Title: _____

Phone: _____

E-Mail: _____

Mailing Address: _____

Incident Description

Describe the nature of the breach and its cause. How was the breach discovered and when? Where did it occur?

_____

Steps 1 & 2: Containment & Risk Evaluation

Answer each of the following questions and then, based on those answers, complete the risk evaluation summary.

(1) Containment

Check all the factors that apply:

- The Personal Information has been recovered and all copies are now in our custody and control.
- Confirmation that no copies have been made.
- Confirmation that the Personal Information has been destroyed.
- We believe (but do not have confirmation) that the Personal Information has been destroyed.
- The Personal Information is encrypted.
- The Personal Information was not encrypted.
- Evidence gathered so far suggests that the incident was likely a result of a systemic problem.
- Evidence gathered so far suggests that the incident was likely an isolated incident.

- The Personal Information has not been recovered but the following containment steps have been taken (check all that apply):
  - A remote wipe signal has been sent to the device but no confirmation that the signal was successful has been received
  - A remote wipe signal has been sent to the device and we have confirmation that the signal was successful.
  - Our audit confirms that no one has accessed the content of the portable storage device.
  - We do not have an audit that confirms that no one has accessed the content of the portable storage device.
  - All passwords and system usernames have been changed.

Describe any other containment strategies used:

---

(2) Nature of Personal Information Involved

List all the data elements involved (e.g. name, date of birth, SIN, address, etc.)

- Name
- Address
- Date of birth
- Government ID number (specify)
- SIN
- Financial Information
- Health information
- Personal characteristics
- Other (describe)

---

(3) Relationship

What is the relationship between the recipient of the information and the individuals affected by the breach?

- Stranger
- Employer
- Health authority
- Co-worker
- Unknown
- Other (describe)

---

(4) Cause of the Breach

Based on your initial investigation of the breach, what is your best initial evaluation of the cause of the breach?

- Accident or oversight
- Technical error
- Intentional theft or wrongdoing
- Unauthorized browsing
- Unknown
- Other (describe)

_____

(5) Scope of the Breach

How many people were affected by the breach?

- Very few (less than 10)
- Identified and limited group (>10 and <50)
- Large number of individuals affected (>50)
- Numbers are not known

(6) Foreseeable Harm

Identify the types of harm that may result from the breach. Some relate strictly to the affected individual, but harm may also be caused to the public body and other individuals if notifications do not occur:

- **Identify theft** (most likely when the breach includes loss of SIN, credit card numbers, driver's licence numbers, debit card information etc.)
- **Physical harm** (when the information places any individual at risk of physical harm from stalking or harassment)
- **Hurt, humiliation, damage to reputation** (associated with the loss of information such as health information, disciplinary records)
- **Loss of business or employment opportunities** (usually as a result of damage to reputation to an individual)
- **Breach of contractual obligations** (contractual provisions may require notification of third parties in the case of a data loss or privacy breach)
- **Future breaches due to technical failures** (notification to the manufacturer may be necessary if a recall is warranted and/or to prevent a future breach by other users)
- **Failure to meet professional standards or certification standards** (notification may be required to a professional regulatory body or certification authority)
- **Other** (specify)

_____

(7) Other Factors

The nature of the Regulator's relationship with the affected individuals may be such that the Regulator wishes provide notification of the breach regardless of the factors are because of the importance of preserving trust in the relationship. Consider the type of individuals that were affected by the breach

- Registrant
- Employee
- Complainant
- Volunteer
- Other (describe)

Risk Evaluation Summary:

For each of the factors reviewed above, determine the risk rating.

Risk Factor	**Risk Rating**		
	Low	Medium	High
1) Containment			
2) Nature of the Personal Information			
3) Relationship			
4) Cause of the breach			
5) Scope of the breach			
6) Foreseeable harm from the breach			
7) Other factors			
Overall Risk Rating			

Use the risk rating to help decide whether notification is necessary and to design prevention strategies. Real risk of significant harm from the breach is usually the key factor used in deciding whether or not to notify affected individuals. Step 3 below analyses this in more detail. In general, though, a medium or high-risk rating will always result in notification to the affected individuals. A low-risk rating may also result in notification depending on the unique circumstances of each case.

Step 3: Notification

(1) Should Affected Individuals be Notified?

Once you have completed your overall risk rating, determine whether or not notification of affected individuals is required. If any of the following factors apply, notification should occur.

Consideration	Description	Factor applies
Legislation	Health custodians in Nova Scotia must comply with sections 69 & 70 of the *Personal Health Information Act*.	
Risk of identity theft	Most likely when the breach includes loss of SIN, credit card number, driver's license number, debit card information, etc.	
Risk of physical Harm	When the information places any individual at risk of physical harm from stalking or harassment.	
Risk of hurt, humiliation, damage to reputation	Often associated with the loss of information such as health information or disciplinary records.	
Loss of business or employment opportunities	Where the breach could affect the business reputation of an individual.	
Explanation required	The Regulator may wish to notify if the affected individuals include vulnerable individuals, or where individuals require information to fully understand the events, even when the risks have been assessed as low.	
Reputation of public body	Where the Regulator is concerned that the breach will undermine confidence in the Regulator's ability to regulate the profession, the Regulator may decide to notify in order to ease concerns and to provide clear information regarding the risks and mitigation strategies undertaken, even when risks assessed are low.	

(2) When and how to Notify

When: Notification should occur as soon as possible following a breach. However, if you have contacted law enforcement authorities, you should determine from those authorities whether notification should be delayed in order not to impede a criminal investigation.

How: The preferred method is direct - by phone, letter, email or in person. Indirect notification via website information, posted notices or media should generally only occur where direct notification could cause further harm, is prohibitive in cost, or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.

Considerations Favouring Direct Notification	**Check If Applicable**
The identities of individuals are known	
Current contact information for the affected individuals is available	
Individuals affected by the breach require detailed information in order to properly protect themselves from the harm arising from the breach	
Individuals affected by the breach may have difficulty understanding an indirect notification (due to mental capacity, age, language, etc.)	
Considerations Favouring Indirect Notification	
A very large number of individuals are affected by the breach, such that direct notification could be impractical	
Direct notification could compound the harm to the individuals resulting from the breach	

(3) What to Include in Breach Notifications

The information included in the notice should help the individual to reduce or prevent the harm that could be caused by the breach. Include all the information set out below:

Essential Elements in Breach Notification Letters	**Included**
Date of breach	
Description of breach	
Description of Personal Information affected	
Steps taken so far to control or reduce harm (containment)	
Future steps planned to prevent further privacy breaches	
Steps individuals can take	
Privacy Officer contact information - for further assistance	

Others to Contact

Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider whether the following authorities or organizations should also be informed of the breach:

- police - if theft or crime is suspected;
- insurers or others - if required by contractual obligations;
- professional or other regulatory bodies - if professional or regulatory standards require notification of these bodies;
- other internal or external parties not already notified, as your investigation and risk analysis may have identified other parties impacted by the breach such as Third-Party contractors, internal business units or unions.

Policy Name	Security of Confidential Information of Regulator of Paramedicine of Nova Scotia		
Policy Number:	Administrative – 1.4		
Version Number	1	**Date first Approved:**	09/28/2021
Approved by:	ED/Registrar	**Effective Date:**	09/28/2021
Version Date:	11/15/2024	**Next Review Date:**	

DEFINITIONS

"Access Control" means the permissions assigned to persons or systems that are authorized to access specific resources;

"Board" means the Board of the Regulator;

"Confidential Information" has the meaning as described in the Regulator's "Confidentiality of Nova Scotia Regulator of Paramedicine Information";

"Employee" has the meaning as described in the Regulator's "Confidentiality of Nova Scotia Regulator of Paramedicine Information";

"Personal Information" has the meaning ascribed to it in the Regulator's "Privacy Policy";

"Regulator" means the Nova Scotia Regulator of Paramedicine;

"Third-Party Service Provider" has the meaning as described in the Regulator's "Confidentiality of Nova Scotia Regulator of Paramedicine Information"; and

"Volunteer" has the meaning as described in the Regulator's "Confidentiality of Nova Scotia Regulator of Paramedicine Information".

POLICY STATEMENT

1. This policy applies to all:

    a) Employees;
    b) Volunteers;
    c) Third-Party Service Providers of the Regulator;
    d) Confidential Information of the Regulator, or in its custody or control, in any form including electronic and paper format.

2. The Regulator shall safeguard all Confidential Information within a secure environment.

3. All parties to whom this policy applies must:

    a) protect information from unauthorized access or misuse;
    b) ensure the confidentiality of information;

c) maintain the integrity of information;
d) maintain the availability of information systems and information for service delivery;
e) comply with regulatory, contractual, and legal requirements;
f) maintain physical, logical, environmental and communications security;
g) dispose of information in an appropriate and secure manner when its continued retention is no longer required.

Authorized Users of Confidential Information

4. All users who have access to Confidential Information of the Regulator must:

a) be formally authorized to access such information by the Executive Director/Registrar of the Regulator;
b) be in possession of a unique user identity when accessing any information systems of the Regulator;
c) refrain from disclosing any password associated with their user identity to any person;
d) take all necessary precautions to protect the Confidential Information in their personal possession and Confidential Information must not be copied or transported without consideration of:
    i) the permission to do so;
    ii) the risks associated with loss or information falling into the wrong hands; and
    iii) how the information will be secured during transport to its destination.

Acceptable Use of Information Systems

5. Users accounts on the Regulator computer systems must only be used for the Regulator's business and shall not be used for personal activities during working hours.

6. During breaks or mealtimes, limited personal use is permitted, but use must be legal, honest, and decent while considering the rights and sensitivities of others.

7. Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to the Regulator's systems for which they do not have authorization.

8. Users shall not attach unauthorized devices to their PCs or workstations, unless they have received specific authorization from the Executive Director/Registrar, or their designee.

9. Users shall not download unauthorized software from the Internet onto their PCs or workstations.

10. Unauthorized use of the company's computer system and facilities may constitute grounds for immediate termination of employment or appointment, civil action, and/or criminal prosecution.

Access Control

11. The Regulator will control access to Confidential Information resources that require protection against disclosure or modification.

12. Access controls will exist for all Regulator information technology hardware and software resources, as well as paper files.

13. Users will be provided with controlled access only to the hardware, software, and paper files necessary for them to perform of their job requirements.

14. Only those who are authorized by the Executive Director/Registrar, or their designate, shall access password files on any network infrastructure component, and password files on servers will be monitored for access by unauthorized users.

15. Copying, reading, deleting, or modifying a password file on any computer system is prohibited.

16. Users will not be authorized to log on as a System Administrator, and Users who need this level of access to production systems must request access from the Executive Director/Registrar.

17. Users will be responsible for all transactions occurring during Logon sessions initiated by use of the user's password and ID.

18. Users shall not log on to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

Handling Confidentiality of Information

19. All Users who handle Confidential Information, regardless of the location from which they work, must:

    a) store paper information in a locked filing cabinet or room accessible only to those who have a need to access the information;
    b) protect electronic information via firewalls, encryption, and passwords;
    c) clear their desks of any Confidential Information and secure any confidential information before going home at the end of the day, or when leaving their workspace unattended;
    d) refrain from leaving Confidential Information visible on their computer monitors when they leave their workstations for any period of time;

e) ensure no unauthorized third-party gains access to the Regulator's confidential information by never accessing information on an unauthorized third-party's IT system, and never leaving unsecured hardcopies of documentation unattended at any time.

20. All Users Shall:

a) ensure USB drives or external hard drives that contain Confidential Information are locked when not in use;
b) mark as "confidential" written or electronic documents that contain Confidential Information;
c) dispose of all Confidential Information properly by shredding or burning written documentation;
d) refrain from discussing Confidential Information in public places;
e) use the Regulator's secure e-mail service to transmit Confidential Information to other parties; and
f) before disposing of an old computer, use software programs to wipe out the data contained on the computer or have the hard drive destroyed.

Security of Confidential Information

21. All electronic information must:

a) be stored on the appropriate Regulator computer systems;
b) regularly backed-up so that it can be restored if or when necessary;
c) disposed of in a secure manner; and
d) not be placed on a CD or DVD at any time, and only be placed on a USB flash drive or external drive when there is no other secure method of data transfer, and only if the device is password protected and labelled appropriately as confidential.

User Responsibilities

22. Users are required to report any weaknesses, incidents of misuse or violations associated with the security of the Regulator's Confidential Information.

23. Users shall:

a) comply with all security procedures and policies;
b) protect their user ID and passwords;
c) inform the Executive Director/Registrar, or their designate, of any security questions, issues, problems, or concerns;
d) assist the Executive Director/Registrar, or their designate, in solving security problems;
e) ensure that all IT systems supporting tasks are backed up in a manner that mitigates both the risk of loss and the costs of recovery;

f) be aware of the vulnerabilities of remote access and their obligation to report intrusions, misuse, or abuse to the Executive Director/Registrar, or their designate; and

g) be aware of their obligations in the event that they store, secure, transmit and dispose of Confidential Information of the Regulator.

Regulator's Right to Monitor IT Hardware and Software

24. The Regulator has the right and capability to monitor electronic information created and/or communicated by users using Regulator hardware, software, and networks, including e-mail messages and usage of the Internet.

25. Users of the Regulator's hardware, software, and/or networks should be aware that the Regulator may monitor usage, including, but not limited to patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and users' electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with Regulator policy.

RELATED DOCUMENTS

Adm 1.5 Cyber Security – Protecting Regulator and Personal Devices

DOCUMENT HISTORY ((Date of Reviews. Revisions, etc):

Attachment "A"

Security Policies Agreement

I acknowledge that any violation of this agreement could cause harm to the Regulator and frustrate the Regulator's work. Therefore, as a signatory to this agreement I recognize that unauthorized use and disclosure of Confidential Information my lead to disciplinary action including immediate termination of employment or appointment and/or legal action against me.

I will direct any questions regarding my confidentiality obligations to the Executive Director/Registrar. I have read and understand the above expectations within this agreement and more broadly within the Confidentiality and Privacy Policies of the Regulator and agree to abide by all duties of confidentiality.

I acknowledge that I have received copies of the Regulator of Paramedicine of Nova Scotia's security policies including:

Adm 1.4 – Security of Confidential of Regulator of Paramedicine of Nova Scotia Information
Adm 1.5 – Cyber Security – Protecting Regulator and Personal Devices
Adm 1.6 – Acceptable Internet and Email Use of Regulator Information Technology Systems

I have read and understand the policies. I understand that, if I violate any of these policies, I may be subject to disciplinary action, including termination of employment or appointment and/or legal action against me.

I further understand that I will contact Executive Director/Registrar if I have any questions about any aspect of the Regulator's policies.

Signatory:

_____

Print Name

_____ _____

Signature *Date*

Regulator Staff:

_____

Print Name

_____ _____

Signature *Date*

Policy Name	Cyber Security – Protecting Regulator and Personal Devices		
Policy Number:	Administrative – 1.5		
Version Number	1	**Date first Approved:**	09/28/2021
Approved by:	ED/Registrar	**Effective Date:**	09/28/2021
Version Date:	11/15/2024	**Next Review Date:**	

DEFINITIONS

"Board" means the Board of the Regulator;

"Confidential Information" has the meaning as described in the Regulator's "Confidentiality of Nova Scotia Regulator of Paramedicine Information";

"Employee" has the meaning as described in the Regulator's "Confidentiality of Regulator of Nova Scotia Regulator of Paramedicine Information";

"Personal Information" has the meaning ascribed to it in the Regulator's "Privacy Policy";

"Regulator" means the Nova Scotia Regulator of Paramedicine;

"Third-Party Service Provider" has the meaning as described in the Regulator's "Confidentiality of Nova Scotia Regulator of Paramedicine Information"; and

"Volunteer" has the meaning as described in the Regulator's "Confidentiality of Nova Scotia Regulator of Paramedicine Information".

POLICY STATEMENT

1. This policy applies to all:

    a) Employees;
    b) Volunteers;
    c) Third-Party Service Providers of the Regulator;
    d) Confidential Information of the Regulator, or in its custody or control, in any form including electronic and paper format.

2. All Users are obligated to protect Confidential Information of the Regulator, and to protect all Regulator and Personal Devices that contain Confidential Information.

3. All Users shall keep all Regulator-issued and personal computers containing Confidential Information, including tablets and cell phones, secure.

4. To keep devices secure users must, based upon the technology being utilized:

    a) keep all devices password protected;
    b) choose and upgrade a complete antivirus software;

c) not leave devices exposed or unattended;
d) install security updates of browsers and systems monthly or as soon as updates are available; and
e) log into company accounts and systems through secure and private networks only.

5. Users must avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

6. New users receiving Regulator-issued equipment, will be provided with:

a) devices that have been set up by the IT company designated to support Regulator operations;
b) instructions for password management; and
c) instructions to protect their devices.

Email Security

7. To avoid virus infection or data theft, users must:

a) avoid opening attachments and clicking on links with:

i) content is not adequately explained (e.g. "Watch this video, it's amazing.");
ii) clickbait titles (e.g. offering prizes, advice);

b) check the email address and names of people they received a message from to ensure they are legitimate; and
c) look for inconsistencies or giveaways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks).

8. If a user is unsure whether an email, they received is safe, they must contact the Executive Director/Registrar, or their designate, for direction regarding the email.

Username and Password Identification

9. All users must have a unique username and password to access the Regulator's IT infrastructure.

10. Users' passwords must remain confidential and under no circumstances should they be shared with management or supervisory staff or any other employees.

11. Users must comply with the following rules regarding password creation and maintenance:

a) passwords must be at least eight characters (including capital and lower-case letters, numbers, and symbols) and avoid information that can be easily guessed (e.g. birthdays);

b) passwords should not be written down, and it is recommended that Users avail of a secure password management system;
c) if users need to write down their passwords, they are obligated to keep the paper or digital document confidential and destroy it when their work is done;
d) passwords must be changed every 60 days;
e) User Logon IDs and passwords will be deactivated as soon as possible if the user is terminated, fired, suspended, placed on leave, or otherwise leaves the Regulator; and
f) Users who forget their Microsoft Office 365 password must call the Executive Director/Registrar, or their designate, to have their password reset.

Data Transfers

12. Users must:

a) avoid transferring Confidential Information to other devices or accounts unless absolutely necessary;
b) when transferring Confidential Information use the Regulator's secure email service, TitanFile;
c) ensure that the recipients of the data are properly authorized people or organizations;
d) report scams, privacy breaches and hacking attempts to the Executive Director/Registrar, or their designate; and
e) contact the Executive Director/Registrar, or their designate, if they have any questions or concerns.

Additional Cyber Security Measures

13. To reduce the likelihood of security breaches, users must:

a) turn off their screens and lock their devices when leaving their desks;
b) report stolen or damaged equipment as soon as possible to the Executive Director/Registrar, or their designate;
c) change all account passwords at once when a device is stolen;
d) report a perceived threat or possible security weakness in the Regulator's systems;
e) refrain from downloading suspicious, unauthorized, or illegal software on the Regulator's equipment; and
f) avoid accessing suspicious websites.

Remote Users

14. Remote users must follow the Cyber Security – Protecting Regulator and Personal Devices Policy and are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

15. Remote users must seek advice from the Executive Director/Registrar, or their designate should they have any questions or concerns about data protection or privacy.

RELATED DOCUMENTS

Policy Adm 1.4 Security of Confidential Information of Regulator of Paramedicine of Nova Scotia
Attachment A – Security Policies Agreement

DOCUMENT HISTORY (Date of Reviews. Revisions, etc):

Policy Name	Acceptable Internet and Email Use of Regulator Information Technology Systems		
Policy Number:	Administrative – 1.6		
Version Number	1	**Date first Approved:**	09/28/2021
Approved by:	ED/Registrar	**Effective Date:**	09/28/2021
Version Date:	11/15/2024	**Next Review Date:**	

DEFINITIONS

"Board" means the Board of the Regulator;

"Confidential Information" has the meaning as described in the Regulator's "Confidentiality of Nova Scotia Regulator of Paramedicine Information";

"Employee" has the meaning as described in the Regulator's "Confidentiality of Nova Scotia Regulator of Paramedicine Information";

"Personal Information" has the meaning ascribed to it in the Regulator's "Privacy Policy";

"Regulator" means the Nova Scotia Regulator of Paramedicine;

"Third-Party Service Provider" has the meaning as described in the Regulator's "Confidentiality of Nova Scotia Regulator of Paramedicine Information"; and

"Volunteer" has the meaning as described in the Regulator's "Confidentiality of Nova Scotia Regulator of Paramedicine Information".

POLICY STATEMENT

1. This policy applies to all:

    a) Employees;
    b) Volunteers and their internet access;
    c) Third-Party Service Providers of the Regulator and their internet access; and
    d) information technology equipment owned by the Regulator including but not limited to all information technology and computer equipment (computers, printers, etc.), as well as use of email, the internet, Wi-Fi access points, voice, and mobile computing equipment.

2. Users shall not:

    a) use another user's ID and password to access the Regulator's IT systems;
    b) perform any unauthorized changes to the Regulator's IT systems or information;
    c) attempt to access data that they are not authorized to use or access;

d) connect any non-Regulator authorized device to the Regulator's network or IT systems either virtually or in person;
e) store data on any non-authorized equipment; or
f) give or transfer Regulator data or software to any person or organization outside the Regulator without the authority of the Regulator.

3. The Executive Director/Registrar, or their designate, will ensure that users receive clear directions on the extent and limits of their authority over computer systems and data.

4. Limited personal use of the Regulator's IT systems is permitted provided it does not:

a) affect the individual's performance;
b) in any way harm the Regulator;
c) violate any terms or conditions of any employment, appointment, or contracting agreement; or
d) place the user or the Regulator in violation of legal or other obligations.

5. All users are responsible for their actions on the internet as well as when using email systems.

6. Users shall not:

a) use the internet, e-mails, or text messages for the purposes of engaging in harassment or abuse;
b) use obscenities or disrespectful remarks in communications;
c) access, upload, send or receive data (including images) that may be offensive in any way, including sexually explicit, discriminatory, defamatory, or libelous material;
d) use the Regulator's resources for personal gain or to run a personal business;
e) use the internet or email to engage in play of any kind;
f) use email systems in a way that could affect their reliability or efficiency, such as distributing chain letters or spam;
g) open email attachments that are received from unknown senders, which may contain malware;
h) remove or disable anti-virus software;
i) place on the internet any information relating to the Regulator, modify any information concerning it, or express any opinion about the Regulator, unless they are expressly authorized to do so;
j) send sensitive or Confidential Information via any means other than the Regulator's secure email transfer system, TitanFile, unless permission to do so is first received from the Executive Director/Registrar, or their designate, and the information is protected;
k) forward business email to personal email accounts (for example, a personal Gmail account);

l) make commitments by internet or email on behalf of the Regulator, unless authorized to do so.
m) download copyrighted material such as music media files (MP3), films and videos (non-exhaustive list) without Regulator approval;
n) in any way, violate copyright, database rights, trademarks, or other intellectual property rights;
o) download any software from the internet without the prior consent of the Executive Director/Registrar, or their designate; or
p) connect to a publicly accessible, non-secured internet connection.

7. Users shall only use software that is authorized by the Regulator, on Regulator computer systems.

8. Authorized software must be used in accordance with the software supplier's licensing agreements.

9. Unacceptable email and internet use includes engaging in any activity that is illegal under local, provincial, federal, or international law. For clarity, the following activities are strictly prohibited:

a) attempted or actual infringements of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or by similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" products or other software the use of which is not authorized by the Regulator;
b) unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Regulator or the end user holds no active license;
c) exporting software, technical information, encryption software or technology, in violation of international or regional export control laws;
d) introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.);
e) engaging in fraudulent offers of services originating from any Regulator account;
f) engaging in security breaches or disruptions of network communication;
g) executing any form of network monitoring that intercepts data not intended for the user's host unless this activity is a part of the individual's normal job/duty;
h) circumventing user authentication or security of any host, network, or account;
i) interfering with or denying service to any user other than the user's host (for example, denial of service attack); and
j) using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

RELATED DOCUMENTS

Policy Adm 1.4 Security of Confidential Information of Regulator of Paramedicine of Nova Scotia
Attachment A – Security Policies Agreement

DOCUMENT HISTORY ((Date of Reviews. Revisions, etc):

Policy Name	Conflict of Interest Policy		
Policy Number:	Administrative – 1.7		
Version Number	1	**Date first Approved:**	04/28/2023
Approved by:	ED/Registrar	**Effective Date:**	04/28/2023
Version Date:	11/15/2024	**Next Review Date:**	

DEFINITIONS

"Actual Conflict of Interest" means a situation where an Applicable Person has a private or personal interest that is sufficiently connected to their Regulatory duties and responsibilities such that it influences the exercise of these duties and responsibilities;

"Applicable Person" includes Board members, registrants, Committee members, volunteers, employees, and third-party service providers;

"Perceived Conflict of Interest" means a situation where reasonably well-informed persons could properly have a reasonable belief that an Applicable Person has an actual conflict of interest, even if they do not; and

"Potential Conflict of Interest" means a situation where an Applicable Person has a private or personal interest that could influence the performance of their Regulatory duties or responsibilities, provided that they have not yet exercised that duty or responsibility.

POLICY STATEMENT

1. The Regulator shall conduct all its affairs with integrity and independence. Conflicts of interest, whether Actual, Perceived, or Potential, must not undermined these values.

2. This Policy applies to all Applicable Persons with respect to the affairs of the Regulator and their Regulatory duties and/or responsibilities.

3. This Policy does not apply where an Applicable Person’s interest is so remote or insignificant that it cannot reasonably be regarded as likely to influence the Applicable Person.

4. Applicable Persons shall use this policy to recognize, disclose, manage, and resolve Actual, Perceived, and Potential conflicts of interests.

5. Applicable Persons shall act in ways that preserve and enhance the reputation and integrity of the Regulator.

6. Applicable Persons must perform their Regulatory duties with the best interests of the public and Regulator in mind and put the best interests of the public first.

7. Applicable Persons, whether or not they hold an outside office or employment, shall not place themselves in any conflict-of-interest situation or in a position which raises doubts about their capacity to perform their Regulatory duties in an objective manner.

8. Applicable Persons are required to disclose to the Regulator any personal, business, commercial, financial, or other interest which could be construed to be an Actual, Perceived, or Potential Conflict of Interest.

9. Applicable Persons shall not permit their own interests to interfere with any decisions they may make, or have influence over, regarding the business and operations of the Regulator or decisions made on behalf of the Regulator.

10. Unless authorized to do so by the Regulator in writing, an Applicable Person shall not:

    a) act on behalf of the Regulator, or deal with the Regulator, in any matter where they are in any conflict of interest or appear to be in a conflict of interest; or
    b) use their position with the Regulator to pursue or advance their personal interests or the interests of any person to which they are closely associated.

11. An Applicable Person must not use their relationship with the Regulator to confer a benefit to:

    a) another Applicable Person;
    b) a friend, family member, or business associate of an Applicable Person;
    c) a corporation or partnership in which an Applicable Person has a significant interest; and/or
    d) a person to whom an Applicable Person owes an obligation.

12. If a conflict of interest arises between the private interests of an Applicable Person and the Regulatory duties of that individual, the conflict shall be resolved in favour of the Regulator.

PROCEDURE

13. All Applicable Persons new to the Regulator shall review and sign the Conflict-of-Interest Agreement (See **Attachments A and B**) prior carrying out any Regulatory duties or responsibilities.

14. All Applicable Persons shall review the Conflict-of-Interest Policy of the Regulator prior to attending any meeting or engaging in any actions on behalf of the Regulator.

15. When the Chair of the Board or a Committee asks for conflicts of interest at the beginning of a meeting, all Applicable Persons shall respond appropriately according with their circumstances and this Policy.

16. At the beginning of every meeting, the Chair of the Board, or a Committee, as applicable, shall ask and have recorded in the minutes whether any Applicable Person has a conflict to declare in respect to any agenda item.

17. Notwithstanding the above statement, all parties in a matter before the Board or a Committee of the Regulator may be screened for conflicts of interest prior to a meeting.

18. In the event of an Actual, Perceived, or Potential Conflict of Interest, the Applicable Person shall be recused from the meeting for the duration of the discussion and shall not participate in any the vote on the matter.

19. The minutes of such meeting shall reflect that the Applicable Person(s) in conflict of interest were recused from the discussion and did not vote on the matter.

Recognizing and Disclosing Conflicts

20. An Applicable Person is presumed to have become aware of a conflict of interest at such a time as a reasonable person would have been aware of it.

21. In cases where a conflict cannot be avoided, an Applicable Person must declare a conflict of interest at the earliest opportunity and, at the same time, shall declare the general nature of the conflict.

22. If an Applicable Person is uncertain whether they are in conflict of interest, they must raise the Perceived or Potential conflict with the Board or Committee, as applicable, and the Board or Committee shall determine whether or not a conflict of interest exists.

23. If discussions do not lead to a resolution, whether or not a conflict of interest exists shall be determined by majority vote, and the Applicable Person perceived to be in conflict shall refrain from voting.

24. Where a conflict of interest is discovered after consideration or decision of a matter, it shall be declared to the Board or Committee, as applicable, and appropriately recorded at the first opportunity.

25. If the Board or Committee determines that the involvement of the Applicable Person influenced the decision of the matter, the Board or Committee may re-examine the matter and may rescind, vary, or confirm its decision.

26. Any Applicable Person who perceives another Applicable Person to be in conflict of interest in a matter under consideration shall raise this concern with the Board or Committee, as applicable. If discussions do not lead to a resolution, whether or not a

conflict exists shall be determined by majority vote, and the Applicable Person perceived to be in conflict shall refrain from voting.

Rules About Gifts

27. An Applicable Person may only accept a gift made to them because of their involvement in the Regulator in the following circumstances:

    a) the gift has no more than token value;
    b) it is the normal exchange of hospitality or a customary gesture of courtesy between persons doing business together;
    c) the exchange is lawful and in accordance with local ethical practice and standards; and
    d) the gift could not be construed by an impartial observer as a bribe, pay off or improper or illegal payment.

28. An Applicable Person shall not use the Regulator's property to make a gift, charitable donation, or political contribution to anyone on behalf of the Regulator, and any gift shall have the authorization of the Regulator or a person the Regulator designates.

29. If the acceptance of any gift might give rise to criticism or concern about a conflict of interest, it should be politely declined.

RELATED DOCUMENTS
Attachment A – Examples of Conflicts of Interest
Attachment B – Conflict of Interest Agreement

DOCUMENT HISTORY (Date of Reviews, Revisions, etc):

Attachment A

Examples of Conflicts of interest

When assessing for conflicts of interest, one must recognize that there are different types of interests that may create a conflict. Additionally, conflicts of interest may appear in several different forms.

The types of interests a decision-maker must be aware of are as follows:

- Individual/personal;
- Client;
- Professional;
- Employer;
- Organizational;
- Public;
- Owner;
- Recipients of Paramedic and/or EMR Services; and
- Any other entities where a person may have interests

Conflicts of interest may come in three different forms including:

- Actual;
- Potential; and
- Perceived.

Avoiding actual, potential, and perceived conflicts of interest are fundamental to ensuring the highest level of integrity and public trust.

Potential Conflicts of Interest may arise from situations where a decision-maker:

- knows a party to the decision or their family on a personal level;
- is currently teaching, or has previously taught, a party to the decision, or vice versa;
- is currently supervising, or has previously supervised, a party to the decision, or vice versa;
- works closely with a party to the decision within another context, such as committee work, or another organization; or
- has a financial obligation to a party to the decision or anyone associated with a party to the decision.

Attachment "B"

Conflict of Interest Agreement

This Conflict-of-Interest Agreement is entered into, by the signatory, on the below date. This agreement applies to all Applicable Parties as described in the Regulator's Conflict of Interest Policy.

I have read and been provided with the opportunity to obtain additional information regarding the Regulator's policy on conflicts of interest.

I understand that as a signatory to this agreement that:

- I have a duty to not use my position with the Regulator for any improper purpose;
- I undertake to avoid all situations in which my personal or business interests' conflict, might conflict, or are perceived to conflict with my responsibilities to or duties with the Regulator;
- I shall declare and, if required, remove myself from both the discussion and vote on any matter where I am in an actual, perceived, or potential conflict of interest;
- in the event that I am in a conflict of interest, the conflict and my name shall be recorded in the Minutes; and
- I undertake not to accept gifts, other than those described in policy as acceptable from current or prospective clients or suppliers.

I acknowledge that any violation of this agreement could cause harm to the Regulator and frustrate the Regulator's work. Therefore, as a signatory to this agreement, I recognize that failing to disclose conflicts of interest may lead to disciplinary action including immediate termination of employment or appointment and/or legal action against me.

By signing this document, I have read and understand the above expectations within this agreement and more broadly within the Conflict-of-Interest Policy of the Regulator and agree to abide by its terms.

Signatory:

_____

Print Name

_____ _____

Signature *Date*

Regulator Staff:

_____

Print Name

_____ _____

Signature *Date*