Cybersecurity and Breach Response Policy

Policy Number: G-05.03.00	Next Review Date: 2029
Approved by: NSRDDA Board	Approval Date: February 8, 2026

1. Purpose

The purpose of this policy is to establish a clear approach for the Nova Scotia Regulator of Dentistry and Dental Assisting (NSRDDA) to prevent, detect, and respond to cybersecurity threats and data breaches that may compromise the confidentiality, integrity, or availability of systems and personal information.

2. Scope

This Plan applies to all employees, Board members, Committee members, contractors, and third-party service providers who access the Regulator's information systems or data.

3. Definitions

- **Breach**: Unauthorized access to, or disclosure of, confidential or personal information.
- **Cybersecurity Incident**: Any attempted or actual unauthorized access, use, disclosure, disruption, or destruction of systems or data.

4. Guiding Principles

This following principles underpin the NSRDDA's cybersecurity incident response:

- **Protect the Public and Sensitive Information**: The Regulator's first responsibility is to protect the public interest and maintain the confidentiality and integrity of registrant, complaint, and operational data. We will strive to protect systems and data.
- **Respond Quickly and Effectively**: Incidents will be addressed promptly, with clear roles, timely communication, and practical steps to contain and resolve the issue.
- **Comply with Legal and Regulatory Obligations**: The Regulator will meet all applicable legal requirements, including privacy breach reporting, documentation, and investigation.
- **Communicate Clearly, Respectfully, and Accessibly**: Internal and external communications will be timely, accurate, and respectful, using plain language and accessible formats.
- **Learn, Reflect and Respond**: Every incident will be reviewed so the Regulator can strengthen its systems, policies, and preparedness with a commitment to continuous learning.

5. Responsibilities

Role	Responsibilities
Registrar	• Oversees breach response and ensures compliance with legal obligations
Cybersecurity Lead	• Coordinates technical containment and reporting
All Staff, Volunteers and Contractors	• Must report suspected breaches immediately and comply with security protocols

6. Breach Response Procedure

The Registrar will ensure that a Cybersecurity Incident Response Plan is developed, reviewed and updated annually.

Tabletop Exercises will be conducted every year to test response capacity and coordination.

All new staff and volunteers will receive training on this policy and the NSRDDA's Cybersecurity Incident Response Plan and phishing and cybersecurity breaches as part of their onboarding.

7. Notification Criteria

The Regulator will notify individuals and authorities of a breach when it is reasonable to believe that the breach poses a real risk of significant harm, in accordance with *PIPEDA* or provincial legislation such as the *NS PHIA*. Where feasible, we will ensure that notifications are clear, accessible, and considerate of the needs of diverse audiences.

8. Recordkeeping and Documentation

All incidents and breaches will be documented, and records will be securely stored in accordance with the NSRDDA's privacy and document retention policies.

9. Monitoring and Review

The Chair of the Finance, Audit and Risk Committee and the Registrar will ensure this policy is reviewed as outlined herein or as required by significant operational or environmental changes.

10. Accountability

The Registrar is accountable for ensuring compliance with this policy.