Rural Community of Fundy Shores
31 Malcolm Meehan Road
Musquash NB
E5J 2G2

POLICY TITLE: INCIDENT RESPONSE PLAN – CYBER SECURITY

POLICY NUMBER: 2025 – 03

VERSION NUMBER: APPROVED

DATE APPROVED: OCTOBER 1, 2025

EFFECTIVE DATE: OCTOBER 1, 2025

Purpose:
This response plan describes the Fundy Shores Cyber Security Incident Response Plan. The plan outlines the stakeholders and actions required to ensure that cyber security events and incidents are addressed in a consistent, coordinated and timely manner.

The incident response plan portion of the document is to be distributed to contractors, consultants, all internal users, management team, executives and IT professionals.

Scope:
This incident response plan be documented to provide a well-defined, organized approach for handling any potential threat to computers and data, as well as taking appropriate action when the source of the intrusion or incident at a third party is traced back to Fundy Shores private network. This Incident Response Plan identifies and describes the roles and responsibilities of the Incident Response Team (IRT). The IRT is responsible for putting the plan into action.

Incident Response Team:

Role	Person Name	Phone	Email
Incident Response Leader/Decision Maker Role	Primary - CAO Alternate -	CAO, (506)-693-0207 CAO Afterhours (506)-754-1685/(506)-425-7470	linda.sullivanbrown@fundyshores.ca
Incident Communication Coordinator	Primary – CAO Alternate -	CAO, (506)-693-0207 CAO Afterhours (506)-754-1685/(506)-425-7470	linda.sullivanbrown@fundyshores.ca
Cyber Insurance Coordinator	Primary – CAO Alternate -	CAO, (506)-693-0207 CAO Afterhours (506)-754-	linda.sullivanbrown@fundyshores.ca

		1685/(506)-425-7470	
Cyber Incident Manager/Cyber Insurance Name	Kelsey Tilley – Account Manager Gallagher Insurance CFC Underwriting Limited	Kelsey – (506)-405-1830 CFC information at the back of this document	Kelsey_tilley@ajg.com
IT Support/Administrator Role	BrunNet IT Solutions (MSP)	(506) 450-4561 Ext 1	support@brunnet.com
Legal Council	Steven Veniot	(506)-634-8600	steven.veniot@gormannason.com

The Incident Response Team is established to provide a quick, effective, and orderly response to computer-related incidents such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of personal information, and other events with serious information security implications.

The Incident Response Team's mission is to prevent a serious financial loss, citizen confidence or information assets by providing an immediate, effective, and skillful response to any unexpected event involving computer information systems, networks, or databases.

The Incident Response Team is authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident. The Incident Response Team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings to management and the appropriate authorities, as necessary.

<u>Types of Incidents and Response Levels</u>
There are three response levels that govern our cybersecurity incident management activities. These response levels will dictate the level of coordination required in response to any given cyber security event or incident, including the level of escalation, stakeholder participation and reporting required. Fundy Shores has a cyber insurance policy covering the following clauses outlined in their cyber insurance package at the end of this document.

Many types of computer incidents may require Incident Response Team activation. Some examples include:

- Breach of personal information
- Firewall breach
- Virus outbreak or ease

- Unauthorized system access
- Phishing or Ransomware attack
- Privilege abuse
- Insider data theft

LEVEL 1 - Severity Level: Low

In this state, most incidents are isolated to an individual's account or device within Fundy Shores. Staff are to follow the phases noted in the next section, coordinate a response in accordance with their defined policies and maintain communication with BrunNet IT Solutions. BrunNet will advise and assist with remediation. Cyber Insurance providers will not be notified of low severity incidents as these incidents pertain to spam/phishing emails, or equipment failure.

LEVEL 2 – Severity Level: Medium

This level implies that some coordination may be required with more than one resource within Fundy Shores. Examples of a medium severity level would pertain to an individual's account credentials being leaked (by phishing email, etc.), or malware/virus detection (on a single device). The affected staff members will follow the phases noted in the next section and maintain communication with BrunNet IT Solutions. At this level, appropriate stakeholders will be notified as it pertains to further detection and remediation. BrunNet will advise, but in most cases, the Cyber Insurance provider will only be notified if containment and remediation exercises are unsuccessful.

LEVEL 3 - Severity Level: High

This level indicates that immediate focus and action are required at the highest level. At this level, a response will be fully coordinated with all the IRT and BrunNet IT Solutions. The affected staff members will follow the incident response phases noted below and maintain communication with Brunnet IT Solutions along with notifying senior management. Incident examples of a severity level 3 would include: firewall breach, virus or malware outbreak (multiple affected systems), data theft, privilege abuse, unauthorized system access, etc. Cyber Insurance providers' Incident Response Line will be contacted to speak with a cyber incident manager to coordinate the initial response to work with BrunNet IT Solutions or any other third-party incident response as deemed necessary.

Incident Response Phases

Plan Administration

- Establish Roles & Responsibilities
- Document & Test Procedures
- Train Personnel
- Apply Protective Measures

Rural Community of Fundy Shores
31 Malcolm Meehan Road
Musquash NB
E5J 2G2

Questions to address:

- Has everyone been trained on cyber/security policies?
- Are our security policies recent?
- Has the incident response plan been approved?
- Do the members of the IRT know their roles?
- Have all IRT members participated in mock drills?

Detection & Assessment

- Request our MSP/Cyber Insurance to conduct mitigation analysis
- Engage Cyber Insurance Provider
- Request a detailed assessment from MSP and/or Cyber Insurance

Questions to address:

- When did the event happen?
- How was it discovered?
- Who discovered it?
- Have any other areas been impacted?
- What is the scope of the compromise?
- Does it affect our operations?
- Has the source of the event been discovered?

Containment

- Monitor information sources
- Detect & Recognize Cyber Security Events
- Triage and Prioritize
- Report to MSP/Cyber Insurance

Questions to address:

- What has been done to contain the breach short term?
- What has been done to contain the breach long term?
- Has any malware been discovered?
- Are our devices protected with MFA?
- Are the cloud services we use protected with MFA?
- Have all access credentials been reviewed/changed?
- Have all recent security patches and updates been applied?
- Have artifacts/malware from the attacker been securely removed?

Mitigation & Recovery

- Mitigate (via containment & education) (MSP & Cyber Insurance)
- Restore to Normal Operations

Questions to address:

- When can the systems be returned to production?
- Have systems been patched, hardened, and tested?
- Can the system be restored from a trusted backup?
- Can the system(s) be re-imaged?
- How long will the affected systems be monitored?

Post Incident Activity

- Conduct Post-Event Analysis (MSP & Cyber Insurance)
- Conduct Lessons Learned
- Continuous Improvement

Questions to address:

- Are we approaching cyber security correctly?
- Do we need to amend our security strategy?
- Should staff be trained differently?
- What weakness did the breach exploit?
- What tools will ensure similar attacks / incidents will not reoccur?

Once a potential incident has been reported, our MSP, BrunNet IT Solutions will be responsible for performing the initial assessment, containment, and recovery unless otherwise deemed a 3rd party will be involved as per the Cyber Insurance policy.

The following checklist identifies steps that can be used to facilitate classifying the incident if one in fact has occurred:

- Collection and review of log files.
- Review of installed or running privileged programs.
- Inspection for system file tampering.
- Sniffer or Network Monitoring Programs reports.
- Detection of unauthorized services installed on systems.
- Evidence of password file changes.
- Review system and network configurations.
- Detection for unusual files.

Incident Response Team

Annual incident response testing will be performed to ensure the organization is prepared in the event of a sensitive data breach by coordinating informal testing with staff and IT Service Providers.

Changes to the policy will be made as deemed appropriate based on the outcome of the IRP tests and/or changes in technology and regulatory requirements.

Staff Responsibilities

All Fundy Shores staff must report any suspected or confirmed breach of personal information on individuals to the CAO. In the event the CAO is unavailable, the CAO's Administrative Assistant and BrunNet IT Solutions are to be notified immediately upon discovery. This includes notification received from any third-party service providers or other business partners with whom the organization shares personal information on individuals.

The staff member reporting the suspected breach will assist in acquiring information, preserving evidence, and providing additional assistance as deemed necessary by the CAO or other Incident Response Team members throughout the investigation.

Roles & Responsibilities

The Chief Administrative Officer (CAO) of Fundy Shores is responsible for supporting the application of this policy and ensuring that cybersecurity concerns are addressed properly.
It is the responsibility of any staff member who does not fully understand any aspect of this policy or their role within it, to seek clarification from the CAO and agree to undertake further training as required.

The "Incident Response Plan" is designed to protect Fundy Shores business activities, citizens, suppliers, and vendors. Failure to adhere to the good practice outlined, or to follow any associated procedures may lead to disciplinary action.

Contact:

For more information or if you have any questions about this policy, please contact the Chief Administrative Officer for the Rural Community of Fundy Shores

Maintenance:

Annual incident response testing will be performed to ensure the organization is prepared in the event of a sensitive data breach by coordinating informal testing with staff members and IT Service Providers. Changes to the policy will be made as deemed appropriate based on the outcome of the IRP tests and/or changes in technology and regulatory requirements.

Version Number	Editor	Changes	Date
1.0	Justin Wood (Brunnet IT Solutions)	Initial Draft	18/08/2025
1.1	Linda Sullivan Brown, CAO Fundy Shores	Formatted to reflect Fundy Shores document style. Completed unknown sections, provided insurance information and	18/09/25

		contact information for all involved, minor grammatical changes.	

Approval & Adoption

This Cyber Security Incident Response Plan has been approved by Rural Community of Fundy Shores on October 1, 2025. It shall be implemented and adhered to by all relevant stakeholders to ensure responsible asset stewardship for the benefit of current and future generations.

Annotation for Official Policy Book

This is to certify that the foregoing is a true and accurate copy of the Cyber Security Incident Response Plan for the Rural Community of Fundy Shores, which was adopted by Council at its duly convened meeting held 1st day of the October, 2025.

_____ _____

Linda N. Sullivan Brown
Chief Administrative Officer/Clerk
Rural Community of Fundy Shores

Date

Appendix –

1) Cyber Insurance Contact Information
2) Cyber Insurance Package

Rural Community of Fundy Shores
31 Malcolm Meehan Road
Musquash NB
E5J 2G2

cfc

Are you experiencing a cyber incident?

Our in-house team is ready to help you, 24 hours a day, 365 days a year

Phone

USA (local):
1-844-677-4155

Australia (local):
1800 803 202

UK (local):
0800 975 3034

Rest of World:
+44 (0) 208 798 3134

Canada (local):
1-800-607-1355

OR

CFC app

- **Download**
  Get our free incident response app at time of policy purchase
- **Register**
  Sign up by entering your policy number when prompted
- **Report**
  It takes just a few short clicks through the app

OR

Online

Notify a claim at
www.cfc.com/claims

OR

Email

Send your details to
cyberclaims@cfc.com

How it works

1

Get in touch

Reach out to us right away and provide us with you company name, phone number, policy number, and brief description of the incident.

2

Immediate response

You'll immediately be assigned an experienced cyber claims specialist to guide you through the incident.

3

Proactive management

We'll support you through the entire lifecycle of your claim, getting you back up and running as quickly as possible.