All our energy.
All the time.

MARITIME ELECTRIC
A FORTIS COMPANY

July 4, 2025

Pamela Williams, K.C.
Chair and Chief Executive Officer
Island Regulatory & Appeals Commission
PO Box 577
Charlottetown PE C1A 7L1

Dear Ms. Williams:

Cybersecurity Measures and Safeguarding Customer Information

Thank you for your letter dated June 13, 2025, regarding cybersecurity and the protection of customer information. Maritime Electric Company, Limited ("Maritime Electric") shares the Commission's concern about the recent cybersecurity incident involving Nova Scotia Power and appreciates the opportunity to outline our approach to safeguarding sensitive data.

Maritime Electric maintains a comprehensive Cybersecurity Risk Management Program ("CRMP") aligned with the National Institute of Standards and Technology ("NIST") Cybersecurity Framework. CRMP is a structured initiative designed to continuously assess and improve Maritime Electric's cybersecurity posture. It includes: regular risk assessments and control evaluations; implementation of minimum cybersecurity standards across all systems; and ongoing training for all employees, including onboarding modules and biannual refreshers supported by monthly phishing simulations.

This program is structured around five core pillars:

- Identify: A detailed inventory of all digital assets is maintained, including sensitive customer data, with clearly defined roles and responsibilities for employees, vendors, and contractors involved in data handling and incident response.
- Protect: Access to systems is tightly controlled through network access control and endpoint protection technologies. All laptops and desktops are encrypted using industry-standard encryption technology. Regular backups are performed following the industry standard 3-2-1 backup methodology, which involves three copies of the data, two different media types, and one copy that is stored offsite.

.../2

180 Kent Street • PO Box 1328 • Charlottetown, PE C1A 7N2
telephone 1-800-670-1012 • **fax** 902-629-3665 • **maritimeelectric.com**

- Detect: Multiple advanced monitoring solutions are used to detect anomalies such as unauthorized access or unusual login patterns. By layering multiple independent tools, the Company takes advantage of product strengths and adds redundancy. These solutions provide 24/7 monitoring and can automatically isolate compromised devices.
- Respond: The Company has an updated Incident Response Plan and conducts annual tabletop exercises. Incident response partners, [redacted], are on retainers and familiar with the Company's systems.
- Recover: The recover goal is to ensure that the Company can quickly return to normal business functions while minimizing impact and learning from the event to strengthen future resilience. This includes developing and implementing recovery plans, communicating with stakeholders, and incorporating lessons learned into future planning. This also includes recovering backups (see protect pillar) as well as deploying new hardware as required. Key vendor lists are maintained to facilitate ordering new hardware.

Maritime Electric's Customer Information System does not collect or store customer Social Insurance Numbers ("SINs"). As such, there are no retention policies applicable to SINs within our systems.

Cybersecurity enhancements referenced in the 2025 Capital Budget include:

- Network Access Control ("NAC") Project Refresh: NAC helps control devices connected to the network, whether physically or wirelessly. Through device profiling and authentication attributes, devices are automatically placed into the appropriate network. A NAC solution also provides a way to quarantine unknown devices. The existing NAC solution has been in place for five years and, following other upgrades to the IT network, the Company is upgrading the existing NAC solution.
- Expansion of Endpoint Detection and Response ("EDR") Capabilities: EDR is an advanced cybersecurity solution designed to monitor, detect, and respond to threats on company devices in real time. EDR can be compared to traditional antivirus tools. However, unlike traditional antivirus tools that focus on known threats, EDR provides continuous visibility into device activity, enabling swift identification of suspicious behaviour, such as unauthorized access or unusual data movement. This technology not only alerts the Company's cybersecurity teams to potential breaches but also equips them with tools to investigate and contain incidents quickly, minimizing potential damage. Maritime Electric is fine tuning and enabling additional protection policies throughout 2025 to ensure a high level of protection is provided by the solution.

- Expansion of the [redacted] is used to collect both asset information and passive vulnerability data. Network traffic at each substation [redacted] is captured, analyzed, and reported for vulnerabilities or anomalies. Alerts are configured to notify the IT team of anything requiring investigation.
- Optimize Existing Technology: Maritime Electric has added many new tools in the last several years. In 2025, the IT department will revisit these solutions, investigate further training opportunities, and ensure the maximum benefit is derived from each product. This review will also provide an opportunity for cross-training to increase overall department expertise.

Since the initial CRMP in 2019, the Company has increased its cybersecurity budget to appropriately address an ever-evolving cybersecurity risk. Furthermore, being part of the Fortis Inc. ("Fortis") group of companies provides a strong support system for cybersecurity. Fortis provides minimum standards for each subsidiary in many areas including governance, cybersecurity training, acceptable use and phishing testing. The subsidiaries participate in biweekly technical meetings as well as monthly IT leader meetings. Both groups also meet in person annually to discuss cybersecurity trends and new technologies.

Recent initiatives have included the development of several centers of excellence ("COE") including [redacted]
These COE's meet regularly to generate knowledge that can be shared with the larger group. Fortis also coordinates quarterly cybersecurity progress reporting from each subsidiary and often spearheads services coordination on behalf of the Fortis group of companies including ransom negotiation services.

To assess the effectiveness of the Company's CRMP, a third-party security rating service, [redacted] has been engaged to provide a quantitative assessment of the Company's cybersecurity posture by monitoring external-facing digital assets such as websites, internet protocol addresses and domains. As shown in the screenshot below, Maritime Electric (i.e., black line) achieved a grade of A (i.e., 90-100%), which is well above the industry average (i.e., blue line) rating of B (i.e., 80-90%). A score of A indicates the Company has strong cybersecurity controls in place, good patching and up-to-date practices, few known vulnerabilities, and low exposure to external threats. It's important to note that a score of A does not mean the Company is not vulnerable, just that known risks are well managed.

[redacted]

One of the most common causes of a cybersecurity breach is when an employee clicks on a malicious link. To help employees identify and avoid malicious links, the Company performs a minimum of 12 phishing exercises each year against all employees. These tests encompass an array of topics and are rated on a five-star difficulty in the [redacted] training platform. On average between 40 to 50% of employees report phishing emails as suspicious and [redacted] in a phishing email. The Company achieved its best results over the past 12 months in June 2025 in both categories. Industry averages are 26% for reporting simulated phishing emails and 4.5% for click rates. The Company continues to identify and implement employee education and awareness best practices.

If a Maritime Electric IT or OT network was breached, the Company's Incident Response Team ("IRT") would activate the Incident Response Plan ("IRP"). This comprehensive plan, which was developed [redacted] ensures Maritime Electric can respond quickly and effectively to cybersecurity incidents that might disrupt operations or compromise sensitive data. The IRT includes internal technology experts along with several vendors under retainers to provide external response services and support for both IT and OT networks.

Once detected, incidents are analyzed to determine their cause, impact, and whether they pose a risk to customer data or operations. This includes classifying the event by severity (i.e., Level 1 to 4), with Level 1 being the most critical (e.g., customer data breach or major service outage), and documenting findings. The goal is to stop the spread of the issue; therefore, affected systems may be isolated, malicious software removed, and long-term fixes are identified to prevent recurrence. Then, systems are restored to normal operation, which includes validating that the issue is resolved and that no further risks remain. If customers are affected, Maritime Electric coordinates communication and resolution through designated teams. After resolution, a formal review is conducted to identify lessons learned and improve future responses.

We trust this response provides the Commission with the necessary assurance regarding Maritime Electric's commitment to cybersecurity and the protection of customer information. Should you require any further details or clarification, we would be pleased to provide them.

Yours truly,

MARITIME ELECTRIC

Michelle Francis
Vice President,
Finance & Chief Financial Officer

MF35