Request IR-1:

With respect to privacy policies and procedures, please provide the following documentation. If any of the documents are not available, please provide the reasons for each request.

(a) Privacy training policy and procedures.

(b) Percentage of staff that completed privacy training in 2024 and 2025.

(c) Privacy complaint and inquiries policy and procedures.

(d) Privacy breach response plan and procedures.

Response IR-1:

(a) Please see NSEB IR-09. NS Power maintains an ongoing privacy training and awareness program for employees, with an emphasis on ensuring training for those employees who deal with customer information in the course of their roles. NS Power develops an evolving annual privacy training and awareness plan which outlines the planned activities for the calendar year, which may include communications for the annual "Data Privacy Day", participation in "Cyber Security Awareness Month" and the development of dedicated training and modules with role specific content (i.e. "Privacy for Call Centers"). A representative sample of privacy training materials has been provided as Confidential Attachments 14-18 to NSEB IR-09. A copy of the guidelines that NS Power follows in implementing privacy training is set out at Confidential Attachment 12 to NSEB IR-09.

(b) As noted above, prior to the Incident, NS Power required privacy training for all employees who processed customer or employee personal information in the course of their role (i.e. Customer Care, Human Resources, and other appropriate groups). In 2024, approximately 96% of assigned training modules were completed (as set out in more detail

below). For 2025, approximately 79% of assigned training was completed, though the schedule for completion of these processes was disrupted due to the Incident. As noted above, since the Incident, NS Power has taken steps to enhance its existing privacy awareness program and increase the frequency of training activities to be completed on a quarterly basis. 100 percent of employees who were required to complete training by virtue of their roles and exposure to personal information completed this training for the first quarter of 2026.

(c) A copy of NS Power's privacy complaint and inquiries policy and procedure has been provided as Confidential Attachment 3 to the response to NSEB IR-9**.**

(d) NS Power maintains procedures for the reporting and escalation of the unauthorized access to personal information (including unauthorized access by employees), and requires the reporting of any potential unauthorized access to personal information as soon as possible after discovery, as well as procedures outlining the response to such reported incidents. Copies of NS Power's Privacy Breach Response Procedure, and Privacy Incident Reporting Procedure are set out at Confidential Attachments 6 and 7 to the response to NSEB IR-09. These processes are integrated within, and support NS Power's broader protocol for responding to a larger scale cyber incident, a copy of NS Power's Cyber Incident Response Protocol, which sets out the procedures NS Power follows in the case of a cyber incident (including considerations for incidents that involve personal information, including with respect to notification to affected customers, and reports to appropriate privacy authorities), has been provided as Board Confidential Attachment 8 to NSEB IR-09.

Request IR-2:

With respect to governance and risk management processes addressing privacy risks, please provide the following documentation or information, as applicable. If any of the documents or information is not available, please provide the reasons for each request.

(a) Privacy governance framework.

(b) Publicly available privacy policy at the time of the cybersecurity incident.

(c) Internal privacy policy (if different from any publicly available privacy policy).

(d) Information as to whether Nova Scotia Power had a designated privacy officer prior to the cybersecurity incident and whether contact information for the officer was made publicly available.

(e) Data collection minimization policy and procedures.

(f) Consent management policy and procedures.

(g) Privacy audit plan and dates of any audits of access to personal data of customers implemented by Nova Scotia Power in the 2 years leading up to the cybersecurity incident.

Response IR-2:

(a) A copy of relevant materials which comprise NS Power's suite of policies, procedures and standards at the time of the Incident have been provided as Confidential Attachments 1-12 to NS Power's response to NSEB IR-9.

As noted in the Incident Report (Section 5, and 8.4), NS Power has been working to enhance its overall privacy governance framework and build on its existing privacy program (policy, procedures and standards). The updated framework is informed by the AICPA's Privacy Management Framework (PMF), which is designed to provide a foundation in establishing and operating a comprehensive and effective information privacy program to address privacy obligations and risks, and ensure monitoring and enforcement of the existing privacy programs.

(b) A copy of NS Power's publicly available privacy policy at the time of the Incident has been provided as Attachment 13 to NS Power's response to NSEB IR-9, which sets out NS Power's practices relating to the processing of personal information.

(c) A copy of NS Power's "Privacy and Personal Information Protection Policy" has been provided as Confidential Attachment 1 to NS Power's response to NSEB IR-9.

(d) Yes, NS Power had a designated privacy officer at the time of the cybersecurity incident. Contact information for the privacy officer is made available on the NS Power website (under "Privacy Officer"), and individuals are instructed that they can contact the Privacy Officer by email (at privacy.offer@nspower.ca) or by mail. NS Power also directs individuals to report any privacy concerns through a website portal (Privacy Statement| Nova Scotia Power).

(e-f) NS Power's suite of policies, procedures and standards (particularly the Privacy and Personal Information Protection Policy, and Collection of Personal Information Policy) attached as Confidential Attachments 1 and 2 to NS Power's response to NSEB IR-9 set out its practices relating to data minimization. NS Power manages customer consent for the collection, use and disclosure through its privacy policy, and in alignment with their privacy governance framework, set out in response to (a) above.

(g) NS Power did not conduct a formal audit of access to personal data of customers in the 2 years leading up to the incident. NS Power prohibits employees from accessing personal information of customers without a legitimate business purpose, and maintains identity and access management procedures designed to ensure that employees are not granted access to personal information without a valid business purpose.

NS Power maintains procedures for the reporting and escalation of the unauthorized access to personal information (including unauthorized access by employees), and requires the reporting of any potential unauthorized access to personal information (including by employees) as soon as possible after discovery (a copy of NS Power's Privacy Breach Reporting Procedure has been provided as Exhibit 7 to Confidential Attachment 1 to the response to NSEB IR-9. This policy includes examples of situations that would require reporting, for further investigation including where "a SharePoint site used to store Personal Information is created without access permissions".

NON-CONFIDENTIAL

Request IR-3:

With respect to reporting to regulators, notification to affected individuals, management and communication, please provide the following documentation or information, as applicable. If any of the documents or information is not available, please provide the reasons for each request.

(a) Date that Nova Scotia Power became aware of the cybersecurity incident.

(b) Date that the Office of the Privacy Commissioner of Canada was notified of the cybersecurity incident.

(c) Date(s) that any other privacy regulators were notified of the cybersecurity incident.

(d) Date(s) that affected individuals were notified of the cybersecurity incident.

(e) Template(s) of notification letter(s) to affected individuals.

Response IR-3:

(a-d) See Section 2 and 4 of the Incident Report for details on NS Power's discovery of the Incident, and the relevant regulatory and customer notification timelines.

(e) See Attachment 1 & 2 of IRs filed to NSEB on September 5, 2025, for a copy of the notices sent to current customers who NS Power determined to have been impacted.

Request IR-4:

With respect to collection and retention of customer information, please provide the following documentation or information, as applicable. If any of the documents or information is not available, please provide the reasons for each request.

(a) Collection, retention and destruction of customer information policy and procedures.

(b) Records of customer data destruction activities in the 2 years leading up to the cybersecurity incident.

(c) List of types of personal data types collected about customers and for what purposes.

Response IR-4:

(a) Copies of NS Power's Privacy Policy (which sets out NS Power's practices relating to the collection, use, disclosure, and other processing of personal information), and its internal Privacy and Protection of Personal Information Policy, the "Records and Information Management Standard, and the "Information Management Policy" have been provided as Attachment 13 and Confidential Attachments 1, 9 and 10 to NS Power's response to NSEB IR-9**.**

(b) The Company does not have such records.

(c) As disclosed in NS Power's Privacy Policy (Attachment 13 to NS Power's response to NSEB IR-9), the types of information which NS Power collects and maintains from customers includes:

- Name and contact information (premise and mailing address, email address, telephone number).

- Identifying information such as date of birth and information from government issued identification.

- Payment information (i.e. banking information and/or credit card information)

- Demographic and household information, such as the number of individuals per household and your household heat source.

- NS Power program participation information: As background, NS Power offers its customers certain programs such as the MyEnergy Insights, HEAT Fund, or Critical Customer Communication Program. The impacted information related to these programs consists of personal information that individuals who enrolled in one or more of these programs would have provided to NS Power to enroll in the programs, or information that they received from NS Power in the course of their participation in the programs.

- Customer Account History: This category relates to information associated with an individual's NS Power account that (depending on the individual customer) may have been stored on the impacted servers. Additional details are set out below.

    - Power consumption data (i.e. data obtained from readings from residential power meters, and, in cases where a customer participates in the Smart Meter program, data about the amount of electricity used by a customer's household over specific intervals of time, as well as household power usage patterns).

- Service requests (i.e. customer requests that may include details about the type of service needed—such as new connections, outage reports, meter issues, billing inquiries, or equipment maintenance—along with the service location).

- Customer payment, billing, and credit history (i.e. customer invoices, records of customer payment, customer account standing, and (if applicable) a customer's history of non-payment).

- Customer correspondence (i.e. correspondence that NS Power sends and receives from customers, which varied depending on the individual customers, including responses to voluntary surveys conducted by Nova Scotia Power).

NON-CONFIDENTIAL

Request IR-5:

With respect to measures implemented to mitigate risk to customers from fraud and identity theft following the cybersecurity incident, please provide the following documentation or information, as applicable. If any of the documents or information is not available, please provide the reasons for each request.

(a) Please provide a list of measures taken by Nova Scotia Power to mitigate risks to affected individuals from fraud and identify theft following the cybersecurity incident

(b) Please detail whether any complaints were received by affected individuals related to mitigation measures. If yes, how many, how were they responded to, and average response time.

Response IR-5:

(a) See Section 4 of the Incident Report for information on the measures taken by NS Power to mitigate the risks to affected individuals following the Incident.

(b) NS Power received 1,137 complaints from customers who first contacted a dedicated number to support general questions on the cyber incident, and then wished to speak to NS Power. NS Power attempted to contact all customers within 2-3 business days and as long as we could reach the customer, we were successful. The theme of the complaints was lack of specific information on what was impacted by individual customer, concerns related to the loss of sensitive information, difficulty registering for the credit monitoring and identify theft services, overall communication, and sharing concerns with NS Power's reputation. Please refer to CA IR-10 (ii) for customer complaints tracking information.

Request IR-6:

With respect to whether any third-party service providers were involved in the breach and if yes, whether there were data sharing agreements in place with them. Please provide the following documentation or information, as applicable. If any of the documents or information is not available, please provide the reasons for each request.

(a) Third-party service providers privacy risk assessment policy and procedures

(b) Whether there were any third-party service providers whose services were involved in the cybersecurity incident. If yes, please provide a copy of their contracts related to data sharing.

(c) If any third-party service providers whose services were involved with the cybersecurity incident, dates that they became aware of any breach of personal data and dates that they notified Nova Scotia Power of same.

(d) Please confirm whether any third-party service providers whose services were involved with the cybersecurity incident were audited by Nova Scotia Power in the 2 years leading up to the cybersecurity incident.

Response IR-6:

(a-d) As outlined in Section 2.0 of the Incident Report, the Incident impacted NS Power's own systems. Specifically, the Incident arose from malware being downloaded and installed on NS Power's systems, and did not originate with a compromise of the services or systems of any third-party service providers.

Request IR-7:

With respect to communications with customers relating to cybersecurity related issues, please provide the following documentation or information, as applicable. If any of the documents or information is not available, please provide the reasons for each request.

(a) Access to information requests policy and procedures.

(b) Amount of access to information requests made by customers related to the cybersecurity incident.

(c) Information about whether access to information requests made by customers related to the cybersecurity incident were responded to within 30 days.

(d) Number of accesses to information requests that were not responded to within 30 days (if any).

(e) Number of privacy complaints and inquiries received from customers related to the cybersecurity incident.

(f) Information about whether all customers' privacy complaints and inquiries were responded to related to the cybersecurity incident.

(g) Average amount of time taken to respond to customers' privacy complaints and inquiries related to the cybersecurity incident.

Response IR-7:

(a) NS Power's "Access to Personal Information Procedure" has been provided as Confidential Attachment 4 to NSEB IR-9**.**

(b-d) NS Power employs an established access request response procedure which is designed to ensure a standard response to customer requests. In the immediate aftermath of the Incident, NS Power experienced an unprecedented increase in the volume of access requests and privacy complaints/inquiries (which were often contained in the same request) from customers relating to the Incident (approximately 300). These were received through a variety of forums, and often escalated from both the TransUnion call centre, or the NS Power customer care centre, or in some cases received directly to the privacy officer inbox or regular mail. Given the significant resources that were required to be dedicated towards the incident response efforts, including the ongoing data analysis required to determine the nature and scope of the information contained within the impacted systems, NS Power was not in a position to investigation and respond to a request within 30 days. NS Power did endeavor to provide a response to those requests within 30 days of receipt, and indicated that it would not be possible to complete their request within the 30 day time frame due to the significant resources being dedicated to the Incident response and investigation efforts. The vast majority of requests, inquiries and complaints that were escalated to the privacy office were addressed within 60 days of receipt. NS Power has since returned to a more typical volume of requests.

(e-g) See response to (a) – (d) above. Privacy complaints and inquiries were often inextricable to a customer's access request in relation to the cybersecurity incident, and were treated similarly, rather than separately categorized. In all cases, appropriate responses were provided as soon as feasible given the resource constraints at the time.