1. General

1.1. Purpose

1.1.1. To manage and control the risk to the reliable operation of the Bulk Electric System (BES) located within the service territory footprint of Emera Maine (hereafter referred to as Emera Maine or the Company) from malicious or unintentional attacks on the BES Cyber Systems used to protect and operate the BES.

1.1.2. The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. In order to identify BES Cyber Systems, Emera Maine shall determine whether the BES Cyber Systems perform or support any BES reliability function according to those reliability tasks identified for their reliability function and the corresponding responsibilities as defined in Emera Maine's relationships with other functional entities in the NERC Functional Model.

1.1.3. To detail the commitment and ability of Emera Maine management to incorporate and enforce the NERC Critical Infrastructure Protection (CIP) cyber security standards (CIP-002 to CIP-011).

1.2. Scope

1.2.1. This Policy establishes the principles to be used by Emera Maine for identifying, managing, and protecting *BES Cyber Systems* and their associated control and monitoring systems and information, owned or developed by Emera Maine.

1.2.2. This Policy applies to Emera Maine employees, including contract staff and temporary employees, as well as vendors, and other third parties who have authorized electronic or authorized unescorted physical access to *BES Cyber Systems* and to Emera Maine employees and vendor/service contractor personnel who do not have authorized access to *BES Cyber Systems* but are responsible for actions required to achieve and maintain compliance with NERC Reliability Standards CIP-002 through CIP-011.

1.2.3. The definition of terms used in this Policy appears in Attachment A.

1.2.4. Text contained with [ ] denotes the name of an electronic file documenting an internally developed process for the purpose of complying with a specific NERC CIP requirement or set of requirements.

1.3. Governing Principles

1.3.1. Emera Maine shall protect its BES Cyber Systems, such that, those assets continue to provide correct and reliable control, protection and operation of the Bulk Electric System during periods of normal operation and when subjected to directed intentional or unintentional cyber-attack.

1.3.2. Emera Maine shall protect its BES Cyber Systems when subjected to directed intentional cyber-attack, or other emergency situation(s), for which provisional actions are detailed in various Emera Maine Internal Reliability Processes.

1.3.3. This Policy shall be reviewed and authorized by the Emera Maine Senior Manager assigned with the overall responsibility for the implementation of and adherence to NERC Standards CIP-002 through CIP-011 at least every 15 calendar months and the Company shall retain documentation and records from the previous three calendar years to the present.

2. Security Management Controls

2.1. Cyber Security Policy

2.1.1. Emera Maine shall document and implement a Cyber Security Policy [12.001] that represents Emera Maine's commitment and ability to secure its BES Cyber Systems.

2.1.2. Emera Maine shall ensure that its Cyber Security Policy is available to all personnel who have access to, or are responsible for BES Cyber Systems. (Link to CSP)

2.1.3. Emera Maine's Cyber Security Policy shall be reviewed and approved at least every 15 months by the CIP Senior Manager assigned to lead and manage Emera Maine's implementation and adherence to NERC Reliability Standards CIP-002 through CIP-011.

2.1.4. This Cyber Security Policy includes both Medium Impact Assets, as well as Low Impact BES Cyber System.

2.1.4.1. Emera Maine must implement a Cyber Security Awareness Program for its Low Impact Assets as well as Physical Security Controls, Electronic access controls for LERC's (Low Impact External Routable Connectivity) and ensure that the Cyber Incident response program includes Low Impact BES Cyber Assets.

2.2. CIP Exceptional Circumstances

2.2.1. All CIP Exceptional Circumstances (per the definition) shall be reviewed, approved and documented per its internal reliability process [12.003] by the Senior Manager or an authorized delegate to ensure that the intent of this Policy is met.

2.2.2. CIP Exceptional Circumstances shall be reviewed and approved at least every 15 calendar months by the senior manager responsible for adherence to NERC Standards CIP-002 to CIP-011 to ensure that any and all past and present day exceptions are still required and valid.

2.2.3. Documented CIP Exceptional Circumstances must include an explanation as to why the exception is necessary and any compensating measures.

3. Personnel & Training

3.1. Security Awareness Program

3.1.1. Emera Maine shall establish, maintain and document its security awareness program [12.010] to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis for its Medium Impact BES Cyber Systems.

- This procedure supersedes the Security Awareness Program for Emera Maine's Low Impact BES Cyber Assets. All personnel with authorized cyber or authorized unescorted physical access to Emera Maine's Medium Impact assets have authorized access to Emera Maine's Low Impact BES Cyber Systems by default and will therefore receive quarterly reinforcement message.
- The exception to this rule is access to Emera Maine's System Operations and Server Rooms. Access to these protected areas requires higher scrutiny. Advanced security measures have been implemented before access to these areas is allowed (BES Cyber System specific training, background checks, senior manager approval, etc.)

3.2. Cyber Security Training Program

3.2.1. Emera Maine shall establish, maintain and document a cyber security training program [12.010] and shall ensure that all personnel having authorized access to BES Cyber Systems, including contractors and service vendors are trained prior to being granted access except in an emergency (as detailed in document [12.010]).

3.2.2. Emera Maine's training program [12.010] shall cover:

3.2.2.1. Cyber security policies;
3.2.2.2. Physical access controls;
3.2.2.3. Electronic access controls;
3.2.2.4. The visitor control program;
3.2.2.5. Handling of BES Cyber System Information and its storage;

3.2.2.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan;
3.2.2.7. Recovery plans for BES Cyber Systems;
3.2.2.8. Response to Cyber Security Incidents; and
3.2.2.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with removable media.

3.2.3. After initial training of personnel having granted authorized access to BES Cyber Systems, the Company shall ensure that follow-up training is provided every 15 months to persons with such access and that this activity shall be conducted and documented per its reliability process [12.010].

3.2.4. Emera Maine shall ensure that its cyber security training program [12.010] is reviewed at least every 15 months and updated as necessary.

3.3. Personnel Risk Assessment Program

3.3.1. Emera Maine shall develop and document a personnel risk assessment program [12.010], in accordance with federal, state and local laws, and (subject to existing collective bargaining unit agreements), for personnel (including contractors or service vendors) having authorized cyber or authorized unescorted physical access to BES Cyber Systems.

3.4. Access Management Program

3.4.1. Process to authorize Electronic and/or physical access to protected areas, as well as access to designated BES Cyber System Information Storage locations.

3.4.2. Emera Maine shall maintain and regularly review lists of personnel with authorized cyber or authorized unescorted physical access to BES Cyber Systems, including their specific electronic (a.k.a. logical) and physical access rights to BES Cyber Systems following its internal reliability process [12.010].

3.4.3. Emera Maine shall ensure that maintained lists of personnel with authorized cyber or authorized unescorted physical access to BES Cyber Systems are reviewed and updated of any change of personnel with such access to BES Cyber Systems or any change in the access rights of such personnel. EM shall ensure access

list(s) with names of Emera Maine employees, contractors and service vendors are properly maintained.

3.5. Access Revocation (CIP-004-6 R5)

3.5.1. Emera Maine shall implement a process to initiate removal of an individual's ability for unescorted physical access and cyber access upon a termination action, and complete the removals within 24 hours of the termination action

3.5.2. For reassignments or transfers, Emera Maine shall revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that Emera Maine determines are not necessary by the end of the next calendar day following the date that Emera Maine determines that the individual no longer requires retention of that access.

3.5.3. For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic by the end of the next calendar day following the effective date of the termination action.

4. Electronic Security Perimeters

4.1. Electronic Security Perimeter

4.1.1. Emera Maine shall ensure that every Cyber Asset connected to a network via a routable protocol resides within an Electronic Security Perimeter [12.011] and that it shall identify and document the Electronic Security Perimeter(s) and all access points to these perimeter(s).

4.1.2. Emera Maine shall ensure all External Routable Connectivity must be through an identified Electronic Access Point (EAP).

4.1.3. Emera Maine shall require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.

4.1.4. Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.

4.2. Electronic Access Controls

4.2.1. If Emera Maine allows Interactive Remote Access to BES Cyber Systems Emera Maine shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible.

Physical Security of BES Cyber Systems

4.3. Physical Security Plan

4.3.1. Emera Maine shall document, maintain and implement a physical security plan [12.013] to restrict physical access to its BES Cyber Systems.

4.4. Visitor Control Program

4.4.1. Emera Maine shall implement a visitor control program [12.013] for visitors (personnel without authorized unescorted access to a Physical Security Perimeter) that shall contain logs to document the date and time of entry and exit of visitors to and from Physical Security Perimeters (PSP) and that visitors within a PSP shall be continuously escorted by a person granted authorized unescorted access to the specific PSP.

5. Systems Security Management

5.1. Ports & Services

5.1.1. Emera Maine shall establish, document and implement a process [12.016] to ensure that only those ports and services required for normal and emergency operations are enabled and shall disable other ports and services (including those used for testing purposes) prior to production including port ranges or services where needed to handle dynamic ports.

5.1.2. Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media

5.2. Security Patch Management

5.2.1. Emera Maine shall establish, document and implement a security patch management program [12.017] for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

5.3. Malicious Code Prevention

5.3.1. Emera Maine shall deploy method(s) to deter, detect, or prevent malicious code. [12.018].

5.3.2. Emera Maine shall mitigate the threat of detected malicious code.

5.4. Security Event Monitoring

5.4.1. Emera Maine shall log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents.

5.4.2. Emera Maine shall generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):

5.5. System Access Controls

5.5.1. Emera Maine shall have a method(s) to enforce authentication of interactive user access, where technically feasible. [12.019].

5.5.2. Emera Maine shall Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).

5.5.3. Emera Maine shall identify individuals who have authorized access to shared accounts.

5.5.4. Emera Maine shall change known default passwords, per Cyber Asset capability

5.5.5. Where technically feasible, for password-only authentication for interactive user access, Emera Maine shall either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.

6. Incident Reporting & Response Planning

6.1. Cyber Security Incident Response Plan Specifications

6.1.1. Emera Maine shall develop and maintain a Cyber Security Incident Response Plan [12.024] and implement the plan in response to Cyber Security Incidents. The Company's Cyber Security Incident Response Plan shall address, at a minimum:

- One or more processes to identify, classify, and respond to Cyber Security Incidents.
- One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law.
  - Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.
- The roles and responsibilities of Cyber Security Incident response groups or individuals.
- Incident handling procedures for Cyber Security Incidents.

7. Recovery Plans for BES Cyber Systems

7.1. Recovery Plan Specifications (CIP-009-6 R1)

7.1.1. Emera Maine shall develop and document recovery plans for its BES Cyber Systems that collectively include:

7.1.1.1. Conditions for activation of the recovery plan(s).
7.1.1.2. Roles and responsibilities of responders.
7.1.1.3. One or more processes for the backup and storage of information required to recover BES Cyber System functionality.
7.1.1.4. One or more processes to verify the successful completion of the backup processes in Part 9.1.1.3 and to address any backup failures.

7.1.1.5. One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s).

8. Configuration Change Management and Vulnerability Assessments

8.1. Configuration Change Management

8.1.1. Emera Maine shall develop a baseline configuration, individually or by group, which shall include the following items:

8.1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists;
8.1.1.2. Any commercially available or open-source application software (including version) intentionally installed;
8.1.1.3. Any custom software installed;
8.1.1.4. Any logical network accessible ports; and
8.1.1.5. Any security patches applied.

8.1.2. Emera Maine shall authorize and document changes that deviate from the existing baseline configuration.

8.1.3. For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.

8.2. Vulnerability Assessments

8.2.1. At least once every 15 calendar months, Emera Maine shall conduct a paper or active vulnerability assessment.

8.2.2. Document the results of the assessments conducted according to Parts 10.3.1, and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.

8.3. Transient & Removable Media

8.3.1. For its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, Emera Maine shall implement, except under CIP

Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media

9. Information Protection

9.1. Information Protection

9.1.1. Emera Maine shall document and implement one or more documented information protection program(s) that collectively includes [12.005]

9.1.1.1. Method(s) to identify information that meets the definition of BES Cyber System Information.

9.1.1.2. Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.

Version History

Version	Action	Date
1	Original	June 29, 2011
2	Corrected document references Section I item 3.2 Added language Section IX item 1.1 further specifying Emera Maine actions regarding access to CCAs during emergencies. Added document 12.024 to Related Document List	July 9, 2011
3	Change 2.2 to define applicability of policy to Emera Maine and non-Emera Maine personnel. Define the term “annually” as meaning once each calendar year Clarification of commitment and ability of Emera Maine to protect BES Cyber Systems during emergency situations. Minor grammatical edits Classification level changed from Proprietary to Unrestricted Signatory page changes	December 30, 2011
4	Signatory page change, Gerry Chasse appointed as BHE new President & COO Incorporate Version 3 changes into policy as appropriate	February 23, 2010

	Change all references of BHEC to Emera Maine	
5	Change various references of Version 2 to Version 3 Added Visitor Control program to Physical Security Perimeter Plan (Section VI) per new requirement of CIP-006-3 Added Matt Allen to signatory page and corrected name of Company's President to full name	October 25, 2010
6	Changed all references from "Bangor Hydro" to "Emera Maine" Updated titles on Signatory Page	February 14, 2014
7	Updated hyperlink to CSP on emeramaine.com	April 1, 2014
8	OVERHAUL OF PROCESS • Updated to conform to V5 Standards • Streamlined numbering scheme • Updated signatory page	December 14, 2015
9	Updated to adhere to NERC CIP V6 Standards	February 24, 2016
10	Update to document references	August 25, 2016
11	Updated Document to include Low Impact Assets	March 31, 2017
12	Minor document updates	January 4, 2018

Approvals - Signatures

PREPARED: _____

Date: 1/4/18

Matt Allen

Compliance, Security & Environmental Supervisor

Emera Maine

APPROVED: _____

Date: 01/12/2018

Lois Smith

Sr. Director, IT & Support Operations (CIP Senior Manager)

Emera Maine

APPROVED: _____

Date: 1/5/18

Tim Pease

Director, Legal & Regulatory Affairs (FERC Compliance Officer)

Emera Maine