Title: **CYBER SECURITY POLICY**

Policy Statement: Ontario Power Generation shall operate its information and operational technologies in a secure, vigilant, and resilient manner that minimizes cyber risks to its information assets and generation facilities.

Requirements:

OPG shall establish and maintain a management system that reduces cyber risk, protects critical information and operational technology assets in accordance with internationally recognised cyber security standards, while, at a minimum, maintaining compliance to legal and regulatory requirements.

OPG shall ensure employees, contractors and suppliers are in compliance with all applicable requirements in the management system.

OPG shall foster a culture of awareness that promotes secure practices in the use of all technologies and information assets.

OPG shall take appropriate steps to monitor its information and operational technologies on an ongoing basis to detect, and respond to, threats that impact the confidentiality, integrity, and availability of its assets.

OPG shall ensure strategies are in place to prepare for, respond to, and recover from cyber security incidents that impact its reputation, energy production, and public and employee safety.

OPG shall have a Cyber security Governance Committee comprised of OPG Senior Leaders from Operations, Projects, Information Technology, Legal and Risk to provide management oversight over the cyber security program.

Accountabilities:

The Chief Financial Officer & Corporate Services Officer is accountable for the development and maintenance of a management system for cyber security that achieves the requirements of this policy, including reporting to the Board on OPG's overall cyber security performance.

The Chief Information Officer (CIO) is accountable for the effective implementation of the management system for cyber security of information and operational technologies across OPG's Operating Units and Functions through a center-led function.

The Operating Unit and Function leaders are accountable for complying with the management system for cyber security.

The Cyber security Governance Committee is accountable for identifying cyber risks and risk treatment plans, developing risk appetite statements, recommending risk tolerance levels, and monitoring the cyber security program performance.

All OPG employees are accountable for cyber security and any associated requirements within the scope of their accountabilities.

Sponsoring Unit: Corporate Services Office **Approval:** Board of Directors

Effective Date: January 31, 2025

Document requires CNSC Notification ☑