FORTIS INC.

# Technology Acceptable Use Policy

## Introduction

At Fortis Inc. ("**Fortis**") we realize the importance of cyber security in enabling achievement of our business objectives and are therefore committed to the security and protection of our information technology (**IT**) resources.

This policy prescribes the standards and rules to be followed by Fortis employees when using Fortis IT resources.

## Definitions

"**Employee(s)**" means Fortis employee(s).

"**IT Resources**" mean all Fortis systems, resources and deployed equipment, including but not limited to computer equipment, servers, routers, printers, copiers, facsimile machines, software, operating systems, storage media, network accounts providing electronic mail, and corporate-owned mobile devices.

## Technology Acceptable Use Policy

**1.** IT Resources are used for conducting Fortis business. Reasonable incidental personal use is permitted provided it does not interfere with the performance of work-related duties.

**2.** Employees must not engage in any activity that is illegal under local, provincial, federal, or international law while using IT Resources.

**3.** Use of IT Resources for personal profit is prohibited.

**4.** Employees should have no expectation of privacy in their use of IT Resources. All IT Resources are the property of Fortis and can be monitored and/or searched for policy compliance and enforcement.

**5.** Using IT Resources to view, procure or transmit material that is in violation of sexual harassment or hostile workplace laws or Fortis policies is prohibited. In this regard, Employees should consult the Fortis *Code of Conduct* and *Respectful Workplace Policy*.

6. Providing private personal information regarding Employees to third parties for non-Fortis business is prohibited unless authorized by Fortis's Privacy Officer. In this regard, Employees should consult the Fortis *Privacy Policy*.

7. Disclosing any confidential or proprietary corporate information to any third party without prior authorization and appropriate contractual or other safeguards (as reviewed and approved by the Fortis Legal Department) is strictly prohibited.

8. Employees must not post any information pertaining to Fortis on any public Internet newsgroups, blogs, websites, or bulletin boards, except as authorized and conducted by the Fortis Communications Department.

9. All data created on any IT Resource constitutes Fortis property and must only be stored or reside on Fortis-owned/approved devices. Employees must not transmit Fortis-owned data through or to personal email or unapproved electronic file-sharing mechanisms (e.g., Dropbox, Google Drive, etc.) If there is a business requirement to transmit/copy Fortis-owned data to a cloud-based solution it must be done in consultation with the Fortis Director of Information Systems and Security.

10. Employees must use caution when opening electronic mail attachments, regardless of sender, to safeguard against inadvertently introducing viruses or other forms of malware to the IT Resources environment. For more information, Employees are directed to consult the Fortis IT Department on how to monitor for such risks.

11. Employees must not install software or modify hardware within the IT Resources environment without prior authorization from the Fortis IT Department.

12. Non-Fortis owned assets, including employee-owned personal devices, must not connect to IT Resources without the prior written permission of the Fortis Director of Information Systems and Security.

13. Employees must complete annually prescribed, mandatory Cyber Security Awareness computer-based training.

14. Employees must not seek to gain unauthorized access to, circumvent or attempt to circumvent any security controls implemented to protect IT Resources.

15. Employees must notify the Fortis IT Department if they know of or suspect any risks that could expose Fortis data or information to loss, damage or unauthorized access (e.g., compromised user credentials, stolen assets, phishing, etc.)

16. Employees must not connect any personally owned or removeable storage media (e.g., USB drives, thumb drives, etc.) from untrusted sources to any IT Resource. Employees requiring removable storage media for business purposes should consult the Fortis IT Department.

17. Employees must use appropriate authentication methods to protect all corporate data and information. This includes but is not limited to complex passwords that are unique to each system, and multifactor authentication mechanisms (e.g., an authenticator app) when available.

18. Employees must securely manage and protect authentication information provided to or used by them, including but not limited to usernames, passwords, building access cards and multifactor authentication mechanisms. These items are not to be shared with others.

19. Employee must take all necessary precautions to protect company information when using a Fortis device when working outside of a company-owned facility, such as working from home or a public location.

## Policy Review

This policy shall be reviewed annually. All policy revisions shall be approved by the Fortis VP, CIO and Director of Information Systems and Security.