inter pipeline

# *Cybersecurity Policy*

Inter Pipeline Ltd. ("Inter Pipeline") will manage information systems and electronic information in a manner that will promote Inter Pipeline's corporate vision and strategic goals by ensuring that confidentiality, integrity, availability and safety is maintained while meeting or exceeding, legislative, regulatory and audit requirements, as well as, shareholder expectations.

Cybersecurity is a shared responsibility and this policy applies across the North American organization, including both corporate and industrial control system (ICS) environments, to all employees, and applicable consultants and contractors. Third party service providers, business partners and vendors who use Inter Pipeline's Electronic Information and Communication Tools (ECT) will be required to have in place, or adopt, robust cybersecurity measures.

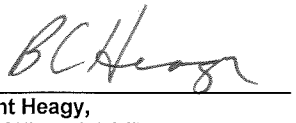
## *Values*

- **System Security –** Implementing cybersecurity functions that allow for safe and secure business activities without unreasonably restricting effective business practices or productivity
- **Threat Response** – Achieving business success through the rapid response to threats and adapting to new technologies and emerging risks
- **Clarity –** Developing and implementing clear policies, standards and procedures that can be exercised, validated and measured
- **Education –** Mitigating cybersecurity risk to the organization through appropriate awareness and training

## *Commitments*

Inter Pipeline will:

- Regularly communicate this policy and other supporting standards, processes, procedures and guidelines as appropriate to ensure strong understanding across the organization
- Ensure that all individuals are able to understand how their behaviour impacts cybersecurity at Inter Pipeline by providing appropriate cybersecurity awareness and training
- Utilize industry partnerships and existing cybersecurity methods, standards, procedures and frameworks that foster continuous improvement of Inter Pipeline cybersecurity measures
- Take reasonable steps to manage electronic information and records in an efficient, secure and effective manner
- Implement processes to classify all electronic information so that appropriate requirements and controls can be applied to protect it
- Ensure that access to and use of ECT be controlled with appropriate role-based access control measures and appropriately manage and protect all ECT infrastructure and applications from threats and vulnerabilities based on risk to the organization
- Implement appropriate monitoring of ECT activities and cybersecurity events, including breaches of security safeguards, to detect unauthorized electronic information processing activities within the organization
- Implement a reporting process for all incidents affecting the security of ECT, together with appropriate escalation and management decision making processes to ensure a quick and effective response
- Establish a framework to ensure that cybersecurity requirements are identified, assessed and implemented as an integral part of any design, development, implementation of, enhancement to, or acquisition of any new or existing application, data or ECT
- Adopt a risk based approach to the evaluation of third party service providers, business partners, vendors, consultants, contractors and agents to ensure that their practices are adequate to protect ECT, including considering broader initiatives that may include requiring contractual compliance with cybersecurity measures that meet or exceed those imposed by law or Inter Pipeline
- Implement such policies, standards, procedures and guidelines as may be necessary to give effect to the values and commitments expressed in this policy.



**Brent Heagy,**
Chief Financial Officer
Inter Pipeline Ltd.
January, 2018