# CORPORATE SECURITY POLICY

## I. PURPOSE OF THE POLICY

Pembina is committed to protecting its people, information, and assets; complying with legal and regulatory requirements; and meeting industry standards and best practices.

This Policy is designed to ensure the implementation of risk-based protocols that effectively mitigate threats of intentional harm against the Company's Employees, Contractors, facilities, physical infrastructure, and physical property; and to ensure full compliance with all applicable security regulations and standards.

## II. SCOPE AND APPLICATION

This Policy applies to all officers, employees, consultants, contractors and directors of Pembina and its subsidiaries ("Personnel").

### Definitions

In this Policy:

"**Company**" means Pembina Pipeline Corporation and its subsidiaries;

"**Contractor**" means any individual or entity that is not a Pembina employee and that is engaged by Pembina to perform services for Pembina and includes all employees and contractors of individuals or entities engaged by a Contractor to perform services for Pembina;

**"Control"** means any measure, procedure, barrier, technology, action, or object, that is utilized to deter, detect, delay, or respond to an intentional act of harm against Pembina; and has the same meaning as "safeguard" or "countermeasure;"

**"Corporate Security"** means the implementation of safeguards, controls, or countermeasures intended to:

- protect the Company from intentional acts of harm against its Employees, Contractors, facilities, physical infrastructure, and physical property; and
- ensure full compliance with all applicable security regulations and standards.

**"Corporate Security Plan" or "CSP"** means the policies, standards, procedures, guidance, and training developed and implemented to mitigate threats of intentional harm against the Company's Employees, Contractors, facilities, physical infrastructure, and physical property; and to ensure full compliance with all applicable security regulations and standards.

"**Employee**" means any regular full-time, part-time, contract, temporary, casual, co-op, summer and seasonal employee of Pembina;

"**Executive**" means any of the President and/or Chief Executive Officer, the Chief Financial Officer, the Senior Vice Presidents, and the Vice Presidents of Pembina Pipeline Corporation;

**“Corporate Security Team”** means the team of security leaders and subject-matter-experts who directly or indirectly report into the Senior Vice President of Corporate Services, and who are responsible to develop and ensure compliance with the CSP.

“**Pembina**” means collectively, the Corporation and its subsidiaries;

"**Pembina Worksite**" means any place where Pembina conducts business, including, without limitation, property, buildings, equipment, road systems and Pembina Vehicles, whether owned, leased or rented;

“**Policy**” means this Corporate Security Policy;

# III. PRINCIPLES

## Leadership

Executives, managers, and supervisors – in collaboration with the Corporate Security Team – are responsible for the following in relation to their people, information, operations, and business activities of their division, department, or unit:

- Ensure that security threats are accurately identified and assessed for risk;
- Ensure full implementation of regulated and non-regulated security Controls that are commensurate with the assessed risk, including all applicable requirements of the CSP;
- Allocate sufficient resources to implement all required Corporate Security Controls;
- Ensure that Employees and Contractors are provided security training and awareness to effectively perform their Corporate Security duties and responsibilities;
- Ensure communication of Corporate Security policies, bulletins, and other Corporate Security information to their leadership teams and frontline personnel, including internal departments and external service providers;
- Ensure that all Employees and Contractors understand the process for reporting security threats, suspicious activities, incidents, deficiencies, and non-compliance with Corporate Security standards and regulations;
- Ensure that all Employee and Contractors are appropriately trained (according to their assigned role) and properly equipped to assess, respond to, and effectively recover from security emergencies and crises, in accordance with Pembina’s Emergency Response Plan (“ERP”);
- Ensure full implementation of corrective action for non-compliance with Corporate Security standards and regulations;
- Delegate their Corporate Security responsibilities when they are absent from the workplace or as otherwise required; and
- Foster innovation and the utilization of technology to minimize costs, operational inefficiencies, and impacts to clients.

## Personnel

All Employees and Contractors shall:

- Comply with this Policy, and all policies, rules, and standards made pursuant to it, including the requirements of the CSP;
- Complete all required training under this Policy and the CSP;
- Report real or perceived security threats, suspicious activities, and non-compliance with Corporate Security regulations and standards according to the processes stipulated in the CSP;
- Review all applicable communications pertaining to their duties and responsibilities under the CSP and any other communication distributed by Pembina regarding emerging or evolving security risks;
- Adhere to all requirements of Pembina's ERP as it applies to Corporate Security threats and incidents;
- Take all reasonable steps to protect Pembina assets in their possession or under their control; and
- Demonstrate security awareness and facilitate a culture of security in the execution of their duties.

### Contractors

- Pembina extends its concern for the protection of its workforce to all Contractors. All Contractors are required to either: (i) abide by this Policy; or (ii) have a substantially similar policy that adheres to or exceeds the principles and standards set out under this Policy. Pembina reserves the right to review any Contractor policies to ensure compliance with this Policy.
- Contractors that do not have a substantially similar policy that adheres to or exceeds the principles and standards set out under this Policy must: (i) acknowledge and agree in writing that they will strictly abide (and cause all of their employees and contractors to abide) by the principles and standards set out under this Policy when providing services to Pembina; (ii) provide a copy of this Policy (including all amendments thereto) to all individuals and entities employed or engaged to perform services for Pembina.

No disciplinary or retaliatory action will be taken against a Pembina Employee or Contractor for reporting non-compliance with security regulations and standards or other security concerns, provided:

- Any non-compliance with regulations and standards is not willful and is reported as soon as reasonably practicable;
- No criminal action has occurred; and
- The Employee or Contractor took reasonable steps to prevent any non-compliance from occurring.

## IV. COMPLIANCE

Personnel must comply with this Policy at all times. Pembina may discipline Personnel who fail to comply with any provision of this Policy. Any breaches of this Policy may result in disciplinary action up to and including termination of employment for cause or termination of engagement without notice, as well as potential civil and criminal sanctions. Determination of the appropriate disciplinary measure will depend on the facts of each case, including the nature of the violation, the existence of prior violations, the response to any prior corrective programs and the seriousness of the violation.

Violations of this Policy should be reported in accordance with Pembina's Whistleblower Policy.

## V. ADMINISTRATION

This Policy shall be administered in accordance with all applicable federal, provincial and local laws and regulations.

## VI. REVIEWED AND APPROVED

The Senior Vice President and Corporate Services Officer is the executive responsible for this Policy**.** This Policy will be reviewed annually by the Senior Vice President and Corporate Services Officer and submitted to the Security Steering Committee for approval.

This Policy was last approved by the Security Committee on September 20, 2018**.**

## VII. RELATED POLICIES

The following policies relate to the subject matter of this Policy:

- Whistleblower Policy
- Cyber Security Policy
- Respectful Workplace Policy
- Code of Ethics Policy

## VIII. SUPPORTING DOCUMENTS

Rules and Conventions in support of this Policy may be created and approved by the Senior Vice President, Corporate Services and the Security Steering Committee. The following support this Policy:

- Security Management Plan
- Corporate Security Plan