INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

I. PURPOSE OF THE POLICY

Pembina Pipeline Corporation (the "Corporation") and all entities controlled by the Corporation (collectively "Pembina") are committed to the highest standards for the protection and use of information technology assets by all officers, and all employees, consultants, contractors and agents (collectively, "Users").

The purpose of this policy is to outline the acceptable use of information technology assets and information at Pembina.

II. SCOPE AND APPLICATION

This policy applies to all individuals who have access to Pembina's information technology assets and information that are either owned, licensed or leased by Pembina.

Information technology assets include, without limitation, any equipment or service provided by Pembina or utilized by Pembina Users that can be used to create, reproduce or distribute information. Examples include, <u>but are not limited to</u>: software (including Cloud (SaaS)), desktop computers, shared drives, document management systems, Digital Communication systems, Internet connections, Mobile Devices, printers, plotters and fax machines.

This Policy and the guidelines set forth pursuant to this Policy are intended to supplement, not replace, all existing laws, regulations, agreements, and contracts that currently apply to those resources.

III. DEFINITIONS

Cloud (Saas) means any information technology service in which data, information, and/or resources are stored or retrieved from the Internet through web-based tools and applications

Corporate Network means the Corporation's private local, wide area, and wireless networks, servers and desktops.

Digital Communications means the Corporation's system for exchanging electronic messages such as email, text messages and instant messages, including attachments.

Internet means the Corporation's connection to the public network outside of Pembina.

IT Group means Pembina's Information Technology Group.

Mobile Devices includes mobile phones, smart phones, tablets, laptops, notebooks, USB and external hard drives or other similar devices.

Offensive Material includes, but is not limited to, pornography, hate literature, obscene materials, materials which contravene human rights legislation, and anything that could be interpreted as a form of sexual or workplace harassment.

Protected Information refers to all information that is personal, proprietary, confidential or restricted.

User ID means a User's digital identity.

IV. POLICY STATEMENT

A. Ownership and General Use

The following rules govern the ownership and general use of Pembina's information technology assets and information:

1. The IT Group must approve **ALL** purchases, installs or utilization of hardware, software and Cloud (SaaS) information technology products for all Users and Pembina service units and business units.

2. All Pembina information/data must only be stored, transmitted or shared through IT approved information technology products.

3. Only approved and authorized Mobile Devices may be connected to the Corporate Network.

4. Users are provided access to the Corporate Network, Internet and Digital Communications services to assist them in performing their duties, which assets are to be used for business purposes only; however, reasonable personal use is permissible provided that such personal use does not interfere with the performance of their duties, is consistent with Pembina policies and is not for financial gain.

5. Pembina reserves the right to filter or restrict access to sites deemed to be inappropriate, which includes, but are not limited to, sites that promote, display or disseminate Offensive Material, gambling, social networking, file and photo sharing, media streaming and sites known for distributing harmful viruses.

6. Users with accounts will only access systems, applications, files and data to which they have been granted access. The ability to inadvertently read, execute, modify, delete or copy information does not imply permission to do so.

7. Users must ensure their use of the Corporate Network, Internet and Digital Communications services is appropriate, lawful and in compliance with applicable corporate and information technology policies.

8. Only authorized Users may post content or create the impression that they are representing, stating opinions, or otherwise making statements on behalf of Pembina on social networking sites, blogs or other Internet sites.

9. Users who are aware of any event which threatens the availability, integrity or confidentiality of Pembina's assets or information, or which breaches Pembina's policies, or is contrary to applicable law, must immediately contact the IT Group.

10. Users must obey all applicable intellectual property rights (e.g., copyright, patent, trademark, license agreement) governing the download, distribution or use of items such as text, graphics, music or software accessed on the Internet or in Digital Communications.

11. Users are held responsible for all Internet and Digital Communications activity performed under their User ID.

12. Users must exercise caution when opening e-mail attachments and avoid opening unsolicited attachments. Users should scan all attachments prior to opening and turn off functions that automatically open e-mail attachments.

13. Users, including remote access Users, must take reasonable precautions to safeguard corporate systems by having up-to-date anti-virus software installed on connected Mobile Devices.

B. Unacceptable Use of Information Technology Assets

In using Pembina's information technology assets and information, User's must not:

(a) share account passwords with others or allow the use of your account or User ID by others;

(b) use personal Digital Communications or Mobile Devices for storing corporate information;

(c) modify corporate-owned and installed hardware and software without prior approval from the IT Group;

(d) purchase or install hardware or software (including Cloud (Saas) products) without prior approval from the IT Group;

(e) intentionally access sites or engage in practices on the Internet that have the potential to bring Pembina into disrepute (e.g., accessing sites which promote, display or disseminate Offensive Material);

(f) solicit, distribute or communicate Offensive Materials via Digital Communications or social networking sites; or

(g) attempt to mask, obscure or falsify their identity or actions while using the Internet or Digital Communications.

C. Use of Mobile Devices

Access Control and Compatibility
To successfully integrate Mobile Devices into the Pembina technology landscape:

(a) the IT Group must enable all connection of Mobile Devices to the Corporate Network and will maintain a list of approved Mobile Devices, related software applications and utilities, which will be reviewed on a semi-annual basis by the IT Group to consider inclusion of additional Mobile Devices and applications;

(b) all Mobile Devices must be registered with the IT Group prior to initial use on the Corporate Network;

(c) Users must ensure that they protect the integrity of corporate, private and confidential business information, including protecting all Mobile Devices with passwords, utilizing a secure socket layer virtual private network (e.g., "SSL", "VPN", "CITRIX") connection when accessing Corporate Networks and adhering to corporate security protocols when using non-corporate devices like home-based personal computers or laptops for accessing Corporate Networks; and

(d) Users of corporate and personal Mobile Devices must also comply with the Security of Endpoint Device Guidelines and Mobile Device Acceptable Use Guidelines.

Mobile Security
The IT Group employs a Mobile Device Management (MDM) solution to enforce policies, monitor usage and remotely wipe lost or stolen Mobile Devices. In order to ensure the security of Mobile Devices:

1. All users of Mobile Devices must employ physical security measures. In the event of a lost or stolen Mobile Device the User must inform the IT Group immediately. The Mobile Device will be remotely wiped of all data and locked to prevent access by anyone other than the IT Group. If the Mobile Device is recovered, it can be provided to the IT Group for re-provisioning.

2. Users, including remote access users, must take precautions to safeguard corporate systems by having up-to-date anti-virus software installed on connected Mobile Devices and adhere to Pembina's Malicious Software Protection Guidelines.

3. Passwords and other Restricted Data (as defined by the Pembina Information Management Policy) are not to be stored unencrypted on Mobile Devices.

4. Users must immediately report to their manager and the IT Group of any known incident of unauthorized access.

5. Users must follow enterprise data removal procedures to permanently erase Pembina specific data from Mobile Devices once their use is no longer required.

6. It is the responsibility of the User to ensure that their personal data on their Mobile Devices is backed up.

D. Systems Monitoring

Users should be aware that their use of Pembina information technology assets and information are not completely private; however, Pembina's policy is to not monitor individual usage of information technology assets and information, unless there is a legitimate business reason or concern to do so.

V. CONSEQUENCES OF NON-COMPLIANCE

Compliance with this Policy is a condition of your employment or contract. Policy violations may result in severe consequences, which could include internal disciplinary action up to and including dismissal for cause or termination of contract.

This Policy was last approved by the Board of Directors on **February 25, 2016**.