CA PECL G05 02 001 O

Rev 1.0 November 2018

INFORMATION SECURITY POLICY

PETRONAS ENERGY CANADA LTD.

DOCUMENT AUTHORIZATION

Approved By:

Name	Kevin Georget
Position	CFO
Date	26-NOV-2018

Document Owner:

Name	Darryle Hawkings
Position	Director, Information & Communication Technology
Date	26-NOV-2018

TABLE OF CONTENTS

Section **Page**

1. Summary Statement

This Policy sets forth the Company's requirements for protecting Information Assets, consistent with the expectations and plans of the Company, and in consideration of PETRONAS Global's' requirements. In addition, this Policy describes the principles of Information & Communications Technology (ICT) business-focused approach to delivering consistent, quality, and timely ICT Services to Users. The Company's information security will be undertaken in a manner to manage risks to the Company, ensuring compliance with applicable law and the Company's policies, standards, procedures, and guidelines.

2. Objectives

The objectives of this Policy are to:

- Define the principles and requirements of acceptable use and describe how these will be implemented across the Company;
- Create a framework such that the User is aware of the Company's expectations and requirements for acceptable use of Information Assets and each User's role in protecting the security and integrity of the same;
- Create a framework where the Company, with each User's cooperation, is able to protect the Computing Environment, effectively manage the risks of unauthorized access, and protect the Company's business and reputation;
- Raise the level of awareness of ICT' primary role to deliver ICT services across the Company;
- Promote a culture of quality and continuous improvement; and
- Communicate to ICT Employees the Company's expectations for the delivery of consistently high-quality ICT services based on business needs.

3. Scope

This Policy applies to Users of the Company's Information Assets and Computing Environment.

4. Definitions

Capitalized terms used herein have their meanings set forth in the Master Glossary.

5. Requirements

5.1 Acceptable Use of Information Assets

5.1.1 Access to Information Assets and Services

User access and use of Information Assets must be primarily for the purpose of conducting work and services for the benefit of the Company. Each User must take precautions to safeguard access to the Computing Environment and his/her activities may be monitored to confirm compliance. Reasonable personal, non-commercial use of the Computing Environment is permitted provided that such use:

- Is consistent with the Company's Policies;
- Does not unduly interfere with the User's work and services for the benefit of the Company;
- Does not expose the Company to additional risk (i.e., reputational, legal, or otherwise) or material cost; and
- Does not make use of any information owned or licensed by the Company.

Unacceptable uses include but are not limited to:

- Using or accessing any Information Assets contrary to the User's permissions or authorizations;
- Revealing passwords to others or allowing use of the User's account by others;
- Acquiring and/or making use of another User's password;
- Using any Information Assets for any purposes or activities in poor taste or contrary to applicable law;
- Making offers of products, items, or services (i.e., fraudulent or otherwise) originating from any Company account;
- Causing or contributing to a Security Breach or disruption of network communication, including introducing a Virus into the Company's network;
- Maliciously accessing or intercepting information for which the User is not an intended recipient;
- Except for ICT Employees, monitoring of data, electronic data traffic, or network communications by any means;
- Port Scanning or security scanning of any kind;
- Circumventing User authentication or security controls;
- Using any program, script, command, or sending messages of any kind, with the intent to interfere with, or disable, a User's terminal session, via any means;
- Use of unauthorized computing devices in the Computing Environment; and
- Posting or distributing confidential, proprietary, or other sensitive Company information outside of the Company for non-business purposes.

5.1.2 Privacy and Personal Information

The privacy and content of personal information will be protected in accordance with the Privacy Policy and applicable law. Each User must exercise good judgment regarding the content and nature of personal information he or she introduces into the Computing Environment.

All personal information and messages introduced into the Computing Environment will be treated in a similar manner as business-related information and messages, and their content and use must be consistent with the Company's Policies. The Company reserves the right to examine personal electronic communications and information in accordance with applicable law.

5.1.3 Third-Party Intellectual Property

Only software approved by the Company in advance may be introduced into the Computing Environment.

Information, software, programs, and other electronic products available to Users may be the intellectual property of a third-party and such items may be subject to Intellectual Property Rights and restrictions that govern their access, distribution, or use.

The following activities are specifically prohibited:

- Violation of the Intellectual Property Rights of any third-party by any means, including, but not limited to, the use, installation, or distribution of Pirated or other software products that are not properly licensed for use;
- Unauthorized copying, representation, or use of copyrighted or trademarked material; and
- Use or modification of a patented item, process, or design without the express permission of the patent holder.

The misuse of third-party intellectual property may expose the User and Company to legal action. Any questions concerning the access, distribution, or use of third-party information, software, programs, and other electronic products should be referred to ICT or the Legal department prior to use.

5.1.4 Email

User's usage of Company email accounts must be appropriate and otherwise consistent with this Policy. Unacceptable uses of email include, but are not limited to:

- Opening unsolicited email attachments without prior scanning;
- Using personal email addresses for the Company's business purposes;
- Sending unsolicited email messages, including the sending of junk mail or other advertising material;
- Sending inappropriate email messages that feature adult, offensive, or other material in poor taste;
- Unauthorized use or forging of email header information;
- Any form of harassment via email including solicitation of email from any other email address, with the intent to harass or to collect replies;
- Sending email messages internally or externally that contain unencrypted, sensitive, corporate information. If any doubt exists, consult your supervisor or ICT; and
- Any activity associated with phishing or emails designed to collect personal information under false pretence.

5.1.5 Voicemail

Unacceptable uses of voicemail will be prevented, including, but not limited to:

- Sharing of voicemail boxes without proper authorization by ICT;
- Creating voicemail boxes without password protection; and
- Voicemail greetings or messages with inappropriate content or language (refer to Acceptable Use Agreement).

5.1.6 Instant Communication

Only Instant Messaging (IM) tools that have been made available or approved in advance by ICT may be used to conduct the Company's business and/or loaded into the Computer Environment. Any such IM tool must have appropriate security.

5.1.7 Internet and Social Media

Any Online Social Activities using the Company's hardware or network must be in accordance with this Policy, the Communications Policy, and the Code of Business Conduct and Ethics.

Unacceptable Online Social Activities include, but are not limited to:

- Disseminating, viewing, downloading, storing, or forwarding adult, offensive, or other material in poor taste;
- Harassment or any form of discrimination;
- Discussion or disclosure of confidential, proprietary, or other sensitive Company information;
- Discussion or disclosure of any internal Company matter that could be damaging to the Company or beneficial to the Company's competitors; and
- Use of the Company's logo, brand, or trademarks, or posting non-Company sponsored videos, media clips, or images that reference the Company.

5.1.8 Cloud Storage and Services

In respect of any of the Company's information, any use or access to cloud or personal network storage or backup must be with the prior express permission of ICT.

5.1.9 File Sharing

In respect of any of the Company's information, any use or access to File Sharing Platforms must be with the prior express permission of ICT.

5.1.10 Removable Media

In respect of the storage or transmittal of any of the Company's information, any use of Removable Media must be in accordance with this Policy and the Information Management Policy. Users will obtain approved Removable Media from ICT.

5.1.11 Remote Access

Remote access to the Computing Environment will be provided by the Company to authorized Users. Users must utilize an ICT-approved connection when accessing the Computing Environment from offsite locations. Users must take reasonable precautions to safeguard access to the Company's information and network while using remote access.

5.1.12 Business Applications and Software

All use of business applications and software must be consistent with this Policy and any specific rules defined by each department.

All business applications and software must:

- Have a clear business purpose;
- Have been approved for use by ICT in accordance with this Policy;
- Have been scanned for Viruses;
- Be compatible with the Company's technology and security infrastructure; and
- Be properly licensed and issued in accordance with the distributor's software license (i.e., which itself has been approved in advance by ICT).

Information stored within the business application is considered and will be treated as the Company's proprietary information.

5.1.13 Corporate Mobile Devices

At the Company's discretion, Corporate Mobile Devices will be issued to a User based on his/her job description, role, and departmental approval.

ICT will maintain a list of approved Corporate Mobile Devices and related software applications and utilities.

At its discretion, ICT will install appropriate security measures onto Corporate Mobile Devices. Each User must adhere to this Policy when using a Corporate Mobile Device.

Once use of a Corporate Mobile Device is no longer required or the device is decommissioned, ICT will permanently erase all the Company's information.

5.1.14 Personal Mobile Devices

Users may use Personal Mobile Devices for the Company's business purposes provided that prior ICT approval is obtained before any such device is used in the Computing Environment. ICT will maintain a list of approved Personal Mobile Devices and related software applications and utilities.

Each User must adhere to this Policy when using a Personal Mobile Device.

5.1.15 Lost, Stolen, or Damaged Devices

In respect of a Corporate Mobile Device or Personal Mobile Device where such device contains the Company's information or could be used to access the Company's network or information, Users must immediately report to their supervisor and ICT:

- The loss or theft of such device or of the device's access password or PIN;
- Any incident (real or suspected) to hack or otherwise gain control of such device or access information; and
- Any significant damage to or malfunction of such device.

Refer to the ICT Incident and Service Request Management Framework for additional information. As determined by ICT, appropriate measures will be taken to erase all the Company's data from any compromised device or the Computing Environment and lock them to prevent access by anyone other than ICT. In many circumstances, personal and Company information may be indistinguishable or such measures may otherwise result in the loss of personal information. Users are encouraged to remove or back up such personal information regularly as the Company does not take responsibility for backup of personal information.

5.2 User Accountability

Any real or perceived Security Breach or misuse in relation to Information Assets contrary to this Policy will be reviewed or investigated, and the User may be subject to disciplinary action (up to and including termination of employment or contract) and/or legal action. It is important for each User to understand and accept his/her personal responsibility in the security and integrity of Information Assets and the potentially severe consequences of misuse, loss, and breach of security and confidentiality.

Each User will be required to review and acknowledge this Policy and the Acceptable Use Agreement prior to using or gaining access to the Company's Information Assets and Computing Environment and periodically thereafter as determined by the Company.

5.3 ICT Strategy and Foundation

5.3.1 ICT Strategy

ICT will establish an ICT Strategy in alignment with the Company's Long Term Strategy, and in accordance with the Risk Policy. The objectives of the ICT Strategy will include, but are not limited to:

- Vision for ICT, and establishing the principles for ICT governance and service delivery procedures and guidelines;
- Understanding business needs and creating Service Delivery to meet those needs; and
- Identifying and addressing risks, issues, and prioritized areas for improvement in Information Architecture and Security Architecture reviews and other compliance assessments.

ICT must formulate business cases for strategic asset and services investments, in accordance with the ICT Strategy.

5.3.2 ICT Services

ICT will continuously assess ICT Services and the business activities they support to identify areas of improvement and to understand the need for new or redesigned IT Services.

5.4 ICT Allocation of Responsibilities

5.4.1 ICT Organization and Governance Structure

ICT will create an organization and governance structure to provide:

- Roles and Responsibilities: Defined scope of internal and external decision-making capabilities, functions, and roles, including those ICT activities performed by third-parties;
- Management: Leadership and management for all ICT activities;
- Compliance: Segregation of Duties and compliance assessments of relevant controls under ICT' mandate;
- ICT Infrastructure Services: Computing Environment communications and collaboration;
- ICT Client Services: User support and maintenance of all User devices;
- ICT Application Services: Coordination of all business applications and associated services;
- Information Management: Information Management strategies including information classification, life cycle, and records management, in accordance with the Information Management Policy; and
- Shared Services: Creation and oversight of IT Services related to project management, security, IT applications, business continuity, budgeting and planning, and vendor contract management.

5.4.2 Segregation of Duties

Specific IT Services and Users must be segregated appropriately on the network. For example, access rights will only be granted to defined authorized areas of the Computing Environment.

Roles and responsibilities must be appropriately segregated based on required duties, to prevent fraud and intentional or unintentional misuse of the Computing Environment. Roles and responsibilities must be documented in alignment with ICT Roles and Responsibilities Guideline.

5.5 Information Asset Management

5.5.1 Information Asset Life Cycle Management

Information Assets must be appropriately managed in accordance with the ICT Asset Management Standard throughout the Information Asset management life cycle. All critical assets must be identified and monitored on a regular basis by examining incident trends and, where necessary, taking action to repair or replace.

5.5.2 Asset Acquisition, Development and Maintenance

ICT will create guidelines for the acquisition of Information Assets which take into account future flexibility for capacity additions, obsolescence, transition costs, risks, and upgrades over the Information Asset management life cycle.

All software and technology acquisitions will be done in accordance with the ICT Asset Management Standard.

Maintenance of Information Assets will include periodic reviews of business needs and operational requirements such as patch management, upgrade strategies, risks, vulnerability assessments, and security requirements.

5.5.3 Information Asset Classification and Control

Information Assets will be classified into Asset Categories and assigned to appropriate Information Owners in accordance with the Information Management Policy. ICT will maintain an inventory of Information Assets.

5.5.4 Information Asset Physical and Environmental Security

ICT will put in place all necessary provisions to prevent unauthorised physical access to Information Assets, including risks associated with mobile devices, in accordance with the ICT Access Management Framework. ICT will ensure that Information Assets and their associated housings are physically protected from environmental threats and hazards, in accordance with the ICT Asset Management Standard.

5.5.5 Management of Lost, Stolen or Damaged Assets

Reporting, recording, and resolution of non-routine occurrences like damaged, compromised, lost, or stolen Information Assets will be managed in accordance with the ICT Incident and Service Request Management Framework.

5.5.6 Disposal of Information Assets

Disposal of Information Assets must comply with all regulatory and environmental requirements, in accordance with the ICT Asset Management Standard.

5.5.7 Procurement Practices

Information Assets may only be procured for approved requests, in accordance with the Supply Chain Management Policy and related standards. ICT must follow the AFE Approval Standard, Contract Approval Standard and Invoice Approval Standard to obtain all required approvals during the procurement process. Software and technology solutions will be acquired in accordance with the ICT Strategy, as appropriate.

5.5.8 Planning and Budgeting

ICT must create plans and budgets that demonstrate cost controls, efficiency, and transparency, and also considers quantitative impact, in accordance with the Company's budgeting and accounting policies. Costs within ICT'S control will be actively managed and reported, as required.

5.5.9 Change Management

If changes to existing or new technology solutions result in significant changes to design, functionality, or business processes, then ICT will identify the level of impact and facilitate change adoption, in accordance with the ICT Change Management Framework. Change Management includes:

- Release Management: Collaborating with the Company's management regarding the introduction of new or changed IT Services to align the transition with business needs. This will be done in accordance with the ICT Change Management Framework.
- Configuration Management: Maintaining the configuration of the Information Assets by ensuring authorized components and changes are implemented, in accordance with the ICT Change Management Framework.

5.5.10 Capacity Management

Capacity Management must ensure that Information Assets can deliver service level targets in a cost effective and timely manner. Capacity management will consider short, medium, and long-term requirements, IT infrastructure, and will also consider all other resources required to deliver the ICT services. ICT will proactively monitor and report capacity levels of ICT for the Computing Environment.

5.6 Human Resources Security

ICT will be responsible for creating awareness of information security across the Company for Users upon hiring, during employment, and termination of employment, in accordance with the Talent Acquisition and Deployment Policy.

5.7 Third-Party Contracting

5.7.1 Third-Party Preferred and Ad-Hoc Vendor Contracting

ICT will be responsible for managing all ICT service contracts, including but not limited to, bid proposals and evaluations, awarding contracts, monitoring contractual compliance, and storing contracts in a central repository. Vendor evaluation and pre-qualifications will be conducted in accordance with the Supply Chain Management Policy, and where appropriate, the Talent Acquisition and Deployment Policy.

5.7.2 Managing Contracts

ICT will identify and manage risks in a timely manner to successfully execute and deliver ICT services contracts.

Any amendments to ICT service contracts will be clearly documented and communicated to any affected parties.

ICT service contracts must define and outline criteria to monitor vendor performance, in accordance with the Supply Chain Management Policy.

5.8 Computing Environment

5.8.1 Access Controls

Secure log-on procedures will be employed to prevent unauthorized access to the Company's Information Assets. All access must be authorized by the applicable Information Owner or its delegate. Creation, amendment, and deletion of User Accounts will be done in accordance with the ICT Access Management Framework.

ICT access control is monitored and implemented as follows:

- New User Accounts must have a unique User ID and password, which cannot be reused, and all new User Accounts and passwords must be issued to the Users in a secure manner;
- User Accounts are frequently reviewed to eliminate duplicate or inactive User Accounts and expired access rights to key data and applications;
- Users with Privileged Network Accounts must use a separate User Account that is not a Privileged Network Account for performing normal business functions;
- Users must comply with all password requirements, and ICT will maintain a Password Construction Standard;
- Each User must keep his/her User ID and passwords confidential;
- Default password for Administrative User Account for Commercial Software or databases must be changed upon installation;
- Users must comply with the Acceptable Use Agreement;
- User access privileges will be revoked upon termination of employment or as otherwise deemed appropriate;
- Effective security controls must be employed for remote Users; and
- Access to assets must be physically-restricted to the maximum practical extent possible based on defined asset classification including but not limited to data centres, core infrastructures, and end-user devices.

5.8.2 Operating System, Database and Application Protection

The Company's Computing Environment will be secured as follows:

- Access to the Computing Environment requires secure log-on mechanisms;
- All operating systems, applications, and databases must apply security updates and when it is informed by ICT;
- Access to operating system, database, or application specific utilities and tools that possess the capability to override the existing security controls must be restricted to a limited number of individuals as dictated by business needs and must be approved by ICT; and

- Internet-facing or externally-facing applications will have controls based on the Risk Assessments performed on the relevant areas.

5.8.3 Encryption Protection

Encryption will be utilized as a security measure for protecting Information Assets for the necessary environment.

5.8.4 Firewall Protection

All Internal and External Infrastructure must be segregated by Firewalls to prevent unauthorized access.

5.8.5 Anti-Virus Protection

Anti-Virus Software will be installed on Computing Environment elements that are commonly affected by Viruses. ICT will keep Anti-Virus Software current, actively running, and capable of generating audit logs. All Removable Media will be scanned to check for Viruses, malware, malicious code, and/or inappropriate material.

5.8.6 Spam Email Protection

ICT will scan all incoming and outgoing email for Viruses, malware, malicious code, file attachments, and messages that originate from inappropriate sites or email servers.

5.8.7 Off-Site Data Storage Protection

Information Assets stored off-site will be protected in the same manner as information stored on the Company's internal network in accordance with the Information Management Policy. Selection of off-site storage solutions will go through a Risk Assessment to validate suitability and adherence to the Company's policies.

5.8.8 Interaction / Exchange with Third-Parties

Third-party access to the Computing Environment will only be granted upon approval of a formal access request and execution of the Acceptable Use Agreement.

5.8.9 Mobile Device Protection

Mobile Devices which connect to the Company's Computing Environment must be protected by approved access controls to ensure the Company's Information Assets are secured at all times.

5.8.10 Intrusion Detection

Network intrusion detection system(s) and/or network intrusion prevention solution(s) will be used to monitor all network traffic in the Computing Environment. All implemented intrusion detection and

prevention solutions will be kept up-to-date as appropriate. All identified intrusions must be recorded and reported in accordance with the ICT Incident and Service Request Management Framework. Corrective action will be taken and outcomes will be recorded for future reference.

5.8.11 Security Incident Management

Network vulnerability monitoring of critical IT systems will be performed for the timely identification, reporting, and treatment of vulnerabilities in accordance with the Critical IT Incident Management Framework. This Framework includes incident and critical response steps and provides guidance on:

- Guidance on communication;
- Escalation path for critical incidents;
- Decision-making authority; and
- Steps for identifying and promptly remediating vulnerabilities to minimize Security Breaches associated with vulnerabilities.

5.8.12 Security Breaches

In the event of any real or perceived Security Breach, a User must immediately report to their supervisor and ICT:

- The loss or theft of an Information Asset or of the User Account ID and password;
- Any incident (real or suspected) to hack or otherwise gain control of such Information Asset or the Computing Environment; and
- Any significant damage to Information Assets or the Computing Environment.

As determined by ICT, appropriate measures will be taken to erase all Company data from any compromised device or the Computing Environment and lock them to prevent access by anyone other than ICT. In many circumstances, personal and Company information may be indistinguishable or such measures may otherwise result in the loss of personal information. Users are encouraged to remove or back up such personal information regularly as the Company does not take responsibility for back up of personal information.

5.8.13 Security Assessment and Testing

ICT will conduct regular Security Assessments and testing, with consideration to the outcomes of the ICT Risk Assessment, and incident management and vulnerability management reports.

5.9 ICT Risk Assessment

5.9.1 Risk Assessment

To effectively manage electronic risks, each risk must be identified and assessed through a formal Risk Assessment in accordance with the Risk Policy. ICT will adopt a progressive approach to optimizing information security by implementing suitable controls and other risk mitigation actions.

5.9.2 Risk Tolerance

Risk tolerance criteria and levels will be defined in accordance with the Risk Policy.

5.9.3 Compliance with Applicable Law

All information systems must be designed, operated, and used in compliance with applicable law.

5.10 Business Continuity Management

ICT will identify exposure to Internal and External Infrastructure threats in accordance with the Risk Policy.

5.10.1 Business Continuity Plans and Disaster Recovery Plans

In the event of a disaster, the Business Continuity Plans (BCP) and Disaster Recovery Plan (DRP) may be executed, as appropriate, to meet business and operational continuity requirements.

BCPs and DRPs shall:

- Be included in the systems development life cycle for all systems and applications that have been identified as important or critical, or that have a high availability requirement;
- Be stored in a secure, fire-protected location that is easily accessible with appropriate controls applied, restricting access only to authorized recovery team members; and
- Provide an alternative site or other processing arrangements that are readily available to recover critical ICT functions in the event of disruption or loss of service.

5.10.2 Maintenance and Testing

BCPs and DRPs shall be reviewed, tested, and revised in accordance with a schedule agreed by ICT and the Company's Management.

5.11 ICT Support

ICT will provide quality maintenance support for ICT services and the Computing Environment, in a timely manner.

5.11.1 Acceptable Service Delivery

ICT will manage reporting, recording, and resolution of ICT service issues, in accordance with the ICT Incident and Service Request Management Framework. Support services provided by ICT or third-parties will be continuously monitored and reviewed to ensure they meet the Company's business requirements and priorities for Service Delivery, in accordance with the ICT Strategy.