Purpose

The purpose of this Policy is to communicate how 407 ETR Concession Company Limited and its affiliates (collectively, "**407 ETR**") protects its information systems and information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

This Policy describes steps 407 ETR takes to:

- Reduces business, legal, and regulatory risk;
- Protects its reputation; and
- Ensures the safeguarding and proper use of information, data, computer hardware and other equipment, applications and other software, networks and computer systems at 407 ETR (collectively, "Technology Assets").

Scope and Responsibilities

This Policy applies to 407 ETR employees and, where the context so requires, contractors, consultants, suppliers, representatives and agents of 407 ETR (collectively "**Personnel**") who access or interact with 407 ETR systems.

All Personnel are responsible for ensuring they are familiar with the requirements and guidelines of this policy and applicable procedures.

Policy

407 ETR owns or is the licensee of Technology Assets. They are an integral and important part of 407 ETR's business.

The Technology Assets owned or licensed by 407 ETR are protected under various local and/or international laws, such as patent law, copyright law (including moral rights), trade-mark law, industrial design law, trade secret law, privacy law, as well as other statutory and common law principles ("Intellectual Property Rights"), as may be evidenced by the relevant application, registration, and/or a contract between 407 ETR and a third party. It is 407 ETR's policy to observe and respect all Intellectual Property Rights relating to the Technology Assets. Personnel who do not treat Technology Assets appropriately may be subject to disciplinary action by 407 ETR, up to and including termination. In addition, Intellectual Property Rights owners may take legal action against such Personnel.

407 ETR protects the confidentiality and integrity of information or data stored on its computer systems. To comply with this policy, 407 ETR makes sure that only authorized Personnel have access, appropriate to their duties and responsibilities.

407 ETR ensures effective physical security procedures are in place to protect its Technology Assets from misuse, theft, unauthorized access and disclosure, and various hazards or risks, technological, environmental and otherwise.

407 ETR provides Internet, e-mail and other technology-based business tools to Personnel for the benefit of 407 ETR and its customers. Personnel must not use such tools for, illegal, unethical, or other purposes that may be harmful or prejudicial to 407 ETR.

407 ETR ensures that all of its systems and applications are securely developed and maintained, all production system changes are subject to 407 ETR's Change Management Process.

407 ETR ensures all protected system component logs, including those that perform security functions, are reviewed daily.

407 ETR has a security awareness program which ensures all personnel are aware of the importance of security including cardholder data security. Personnel are required to complete the security awareness program upon hire and annually thereafter.

Policy guidelines

All information, programs, or data its Personnel generate, send, or retrieve using 407 ETR computer systems or Internet connection accounts, is generally considered to be the property of 407 ETR. 407 ETR reserves the right to access such information or data within its computer systems at any time.

This Policy is supported by several underlying policies. All Personnel should be familiar with the requirements of each policy listed below:

Acceptable Use Policy

The purpose of the 030 A - Acceptable Use Policy is to communicate when and where Technology Assets can be used at 407 ETR, and the controls that must be employed when using each technology.

Antivirus Policy

The purpose of the 030 B - Antivirus Policy is to communicate 407 ETR's Antivirus controls and alignment to the Payment Card Industry Data Security Standard (PCI DSS.)

Accounts and Passwords Policy

The purpose of the 030 C - Accounts and Passwords Policy is to communicate the minimum security controls that must be employed at 407 ETR when assigning, using, and maintaining user accounts and their related passwords.

Physical Access Policy

The purpose of the 025 – Physical Access Policy is to communicate how 407 ETR mitigates the risk of unauthorized access to its computers, networks, and information by assigning varying levels of Physical Access to individuals and areas within 407 ETR.

Physical Security

407 ETR uses physical security controls to protect its Technology Assets from misuse, theft, unauthorized access and disclosure, and various hazards or risks, technological, environmental and otherwise.

Physical security controls include, but are not limited to, controlled access to computer and server rooms, logging access to secured rooms, use of CCTV to monitor entrance to controlled areas, and visitor badging procedures.

Only the IT Department installs, disconnects, modifies, and relocates computer equipment. This does not apply to temporary moves or additions of portable computers where the user has already been set up with a computer by the IT Department (e.g. taking a laptop to a meeting room).

Personnel should ensure any portable computing devices such as laptops or PDA devices are properly secured should be secure using IT approved controls. Company-provided laptops should not be left unattended in vehicles.

Keys for offices, laptops, desk drawers, and cabinets that contain Classified Information (as defined in 010 B - Protection of Classified Information) should be securely stored after work hours. Keys should not be "hidden" in any area in Personnel workspace. "Securely stored" refers to either keeping the keys safely in their personal custody or having a secure lockable key cabinet in the department.

When Personnel leave their desk they should always lock their computer screens (e.g. "ctrl", "alt", "delete" for PC users, and activating Hot Corner protection for Mac users).Where possible, laptops should be properly secured to the user's desk using a cable and lock system, which can be obtained from the IT Department and affixed to the desk by the Facilities Department. If a laptop cannot be secured to the desk they should be stored in a securely locked cabinet if the user does not take it home.

Corporate Security

Overall accountability for information security is assigned to the 407 ETR Vice President, Business Process Management.

Responsibilities for the creation and maintenance of security policies, processes and procedures lies with the IT Security Office and Corporate Security Group.

See (Information Security - 407 ETR Organizational Structure)

Observing Intellectual Property Rights

In observing and respecting Intellectual Property Rights related to Technology Assets, Personnel using the Internet must not copy, use, distribute, transmit, or display information, data, or other content protected by copyright laws without first obtaining express permission from the copyright owners.

407 ETR and its Personnel must comply with all applicable intellectual property laws, including, and without limitation, the *Copyright Act*, the *Trade-Marks Act* and the *Patent Act*, as well as any contracts or terms governing the use of Technology Assets, such as licensing agreements or provisions and confidentiality agreements.

The foregoing requirements apply to all Technology Assets that 407 ETR owns or holds rights or a license to, which includes Technology Assets that Personnel, vendors or suppliers developed using 407 ETR resources.

The IT Department must:

- Remove unauthorized software when it is detected/found on 407 ETR devices.

Payment Card Industry - Data Security Standard

All card processing activities and related technologies must comply with the 12 requirements set out in the Payment Card Industry - Data Security Standard (PCI-DSS.)

All PCI requirements are satisfied by the documents listed in the Related Policies and Related Procedures sections below.

407 ETR will adhere to all PCI DSS requirements as established in the PCI DSS.

Exceptions

Any exceptions will be identified and approved as per the process set out in Policy and Procedure Process Guide

Policy Maintenance

Standard maintenance and review as per the process set out in the Policy and Procedure Process Guide

Policy Owner

Chief Information Officer

Related Policies

010 - Record Management and Retention Policy

010 D - Cardholder Data Usage Policy

025 - Physical Access Policy

030 A - Acceptable Use Policy

030 B - Antivirus Policy

030 C - Accounts and Passwords Policy

Related Procedures

N/A

Related Forms

N/A

Related Scripts

Record Retention Schedule

Payment Card Industry - Data Security Standard

Policy and Procedure Process Guide

Information Security - 407 ETR Organizational Structure

Revision History

Date	Version Number	Modifications
December 18, 2003	1.0	Original Version and Date of Issue of the Information Systems Security and Use Policy
August 30, 2005	2.0	Information Systems Security and Use Policy re-issued.
July 24, 2007	3.0	Review of Information Systems and Uses policy, changed to standard Policy format and minor wording edits.
May 22, 2012	4.0	Revised policy to carve out specific PCI related policies and to reference PCI-DSS in this policy as per PCI requirements
July 19, 2013	5.0	Included section on Corporate Security, non-material change, email approval obtained from signatories.
February 14, 2014	6.0	Annual review completed by IT and BPM no material change to content.
April 7, 2015	7.0	Review completed by IT and BPM no changes to content required at this time.
June 30, 2016	8.0	Annual review completed by IT and BPM no material change to content.
April 23, 2018	9.0	Review completed by BPM and IT, no changes identified at this time.

Policy Authorization

Policy Approvers	Approval Date
Jose Tamariz President and Chief Executive Officer	May 22, 2012
Louis-M. St-Maurice Chief Financial Officer	May 18, 2012
Greg Mackenzie General Counsel	May 11, 2012
Robert Ives Chief Information Officer	December 14, 2011
Randy Luyk VP, Business Process Management	December 08, 2011

Note. Completion of the SharePoint workflow by the individuals above is evidence of approval of this document. Workflow approval for this document is available in SharePoint.