Purpose

The purpose of this Protection of Classified Information Policy (this "**Policy**") is to describe the approach to safeguarding Classified Information (as defined below) of 407 International Inc. and its affiliates (collectively,"**407 ETR**"), and to establish guidelines in support of the foregoing, as well as in support of 407 ETR's Records Management and Retention Policy, and Clean Desk Practices and Procedures.

Scope and Responsiblities

This Policy applies to employees, contractors, consultants, suppliers, representatives and agents of 407 ETR (collectively "**Personnel**") who create and/or have access to 407 ETR information.

All Personnel are responsible for ensuring they are familiar with the requirements of this Policy.

Policy

Due to the nature, responsibilities of, and work conducted by various departments, certain documents, data, recorded communications (electronic or otherwise), and other materials (collectively, "**Company Materials**") developed, used, communicated or otherwise identified by the relevant department are deemed to contain "**Classified Information**".

Classified Information is classified into the following categories:

1. "**Protected**" information of the highest level of sensitivity and requires a very high standard of care to protect its confidentiality. Examples of Protected information include:
   - Information that identifies a highly sensitive business transaction, relationship or arrangement, the improper disclosure of which would likely have a material impact on 407 ETR;
   - Credit card numbers; or
   - Information that may be identified by the relevant department and approved by the Corporate Security Group as Protected
2. "**Confidential**" information of a high level of sensitivity and requires a high standard of care to protect its confidentiality. Confidential information may have broad use and availability across 407 ETR**.** Examples of Confidential information include:
   - Information that may provide a competitive advantage to 407 ETR;
   - Non-public information, financial or otherwise, intended for future general, public communication or disclosure;
   - Non-public customer information;
   - Information relating to information technology, including system design, assets and configuration specifications;
   - Internal and external audit information or data; or
   - Information that may be identified by the relevant department and approved by the Corporate Security Group as Confidential
3. "**Internal**" information in Company Materials that is of a sensitive nature and requires a reasonable standard of care to protect its confidentiality. Internal information may

have broad use and availability across 407 ETR. Examples of Internal information or data include:

- Internal management policies and procedures; or
- Internal communications e.g. IT maintenance notifications, HR updates, organizational charts, etc.

4. "**Public**" information is considered to have certain value depending on the circumstances, but there is no risk attributed to unauthorized disclosure. It would not provide a competitive advantage to 407ETR and is routinely made available to interested members of the general public without special restriction. Examples of Public information include:

   - Policies and procedures available on 407etr.com; or
   - Information provided to, or filed with, certain regulatory bodies, e.g. Ontario Securities Commission, via SEDAR

Guidelines

The following guidelines have been established to ensure Classified Information is properly identified and is protected in an appropriate manner.

- Protected and Confidential information should be identified accordingly with the proper description, label, header, or the like where practicable. There is no requirement to label information classified as Internal or Public.
- All hardcopy versions of Protected or Confidential Information should be stored in secured (lockable) filing cabinets within the applicable department. These cabinets must remain locked at all times when not in use, and the keys should be controlled by the responsible Personnel (as determined by the department manager or supervisor), and not made available or provided to any unauthorized individuals.
- Personnel with a separate office must ensure their office doors are locked if it is not practicable for them to use secured filing cabinets.
- All electronic versions of Protected or Confidential Information are stored in 407 ETR's secured database systems. Classified Information attached to or contained in email or other electronic communications should be transferred to a secured database system and removed from an unsecured environment or local email application when practical to do so.
- Passwords used to access the secured database system; email accounts, laptops and other electronic devices must be kept strictly confidential by the responsible Personnel, and not released to any other Personnel.
- Protected, Confidential, or Internal Information must not be stored directly on local hard drives, external devices, or communicated using personal email accounts.
- Disclosure of, or access to, Protected, Confidential, or Internal Information is limited to authorized Personnel. Disclosure of or access to Protected, Confidential, or Internal Information is limited to third parties as authorized by the responsible Personnel, and only on a "need-to-know" basis following execution of a confidentiality agreement by such third party, such agreement to be approved by the Legal Department. The more sensitive the nature of Classified Information (e.g. Protected Information) the more restricted access and disclosure practices should be.

- Personnel may delegate responsibilities concerning access requests and disclosure of Company Materials, as described above, to another individual, appropriate under the circumstances.
- All Company Materials should be disposed of once it is no longer needed, subject to 407 ETR's Records Management and Retention Policy.
- When data may be disclosed or accessible to a third party vendor, a Data Security Form (DSF) must be completed by the business proponent and approved by 407 ETR's Chief Information Officer (CIO) and Privacy Officer. This must occur before the Contract Approval Form (CAF) can commence. The DSF must be completed and approved for all new engagements – for new vendors at time of vendor assessment or selection, and for incumbent vendors at the renewal, extension or re-engagement stage (e.g. each SOW).

Exceptions

Any exceptions will be identified and approved as per the process set out in the 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

VP, Business Process Management

Related Policies

010 - Records Management and Retention Policy

010 A - Clean Desk Practices and Procedures

Related Procedures

010 C - Records Management and Retention Procedures

Related Forms

N/A

Related Scripts

Reccord Retention Schedule

Revision History

Date	Version number	Modifications
February 22, 2013	1.0	Revised Policy to reflect current best practices and accommodate Records Management and Retention Policy. Retitled from Legal Guidelines for Protected information. Previous policy retired.
October 6, 2014	2.0	Annual review completed by BPM no material change to content. Policy ownership changed to VP, BPM from Legal to be consistent with other privacy/information related policy.
February 23, 2016	3.0	Annual review completed by BPM, Legal and IT, enhanced definition and categories of information to 4 from the previous 2 levels. Revision of guidelines.
September 26, 2017	4.0	Annual review completed by BPM, no material changes identified.

Policy Authorization

Approvers	**Approval Date**
Jose Tamariz President and Chief Executive Officer	February 23, 2016
Geoffrey Liang Chief Financial Officer	February 18, 2016
Robert Ives Chief Information Officer	February 18, 2016
Greg MacKenzie General Counsel	February 10, 2016
Randy Luyk VP, BPM	February 8, 2016

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.