Purpose

The first control point in accessing 407 ETR's premises and assets are its physical boundaries. Managing these points ensures access to 407 ETR's information, assets, and its employees are protected.

To mitigate the risk of unauthorized access, 407 ETR assigns varying levels of access to individuals and areas within 407 ETR. This Policy describes the access controls that apply to individuals and areas within 407 ETR's premises and 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**"). All personnel are responsible for ensuring they are familiar with the requirements and guidelines of this Policy and applicable procedures.

Policy

407 ETR controls physical access to its premises, Personnel, and assets through the use of a Building Access Control System. Individuals are provided with badges and access appropriate to their role. Access to badges and the badging system is limited to Security and Facilities personnel only.

407 ETR has identified three distinct groups who require specific access to 407 ETR premises and/or property.

1. **Employees are individuals employed on a full or part time basis by 407 ETR.**
    - Employees will be issued photo ID badges with the appropriate level of access. Employees cannot share ID badges.
    - Cards will be programmed to be active for a set period of time before and after the department's normal business hours as determined and authorized by the Senior Manager responsible for the department.
    - Cards must be worn in such a manner that both the cardholder's photo and name are visible at all times.

    ***Note:** Shareholder Representatives and Directors are considered employees for the purposes of this policy and procedures in terms of their ability to move freely in areas that are not deemed sensitive or controlled.

2. **Persons of Interest (POI) are individuals that 407 ETR engages for a continuing or frequent non-permanent period of time. (e.g. this can include onsite vendors, consultants, contractors, cleaning staff, cafeteria staff, or auditors.)**
    - POI will be issued photo ID badges with the appropriate level of access. POI cannot share ID badges.
    - Cards will be programmed to be active for a set period of time before and after the department's normal business hours as determined and authorized by the Senior Manager responsible for the department.
    - In addition POI access cards will have a programmed expiry date corresponding to their engagement with 407 ETR.
    - Cards must be worn in such a manner that both the cardholder's photo and name are visible at all times.

3. **Visitors are individuals who do not require continuing, frequent, and/or internal access to 407 ETR's premises and property.**
    - Visitors will be issued badges in place of photo ID passes without any access rights attached to them. Visitors can not share badges.

- Visitors are the responsibility of the 407 ETR employee who signs them in and employees must accompany visitors at all times as set out in the visitor access guidelines below.
- The badge will display a validation date and must be worn on an easily identifiable "VISITOR" lanyard provided by 407 ETR.
- Passes must be worn in such a manner that the pass is visible at all times.

***Note:** Children 16 years and younger are considered a visitor but are not required to be badged; however an employee must accompany them at all times.
***Note:** Police officers are also considered visitors and must be badged and accompanied.

Policy Guidelines

Employees must:

- question anyone they find in non-public areas not displaying a valid visitor's badge. Alternatively, employees who feel uncomfortable doing this have the option of immediately notifying their supervisor or the Security Officer instead.
- accompany visitors back to the Security Desk so they may be reunited with their host/escort who signed them in.

Hosts must:

- identify all visitors requiring access to the Security Officer, before the visitor arrives
- inform visitors about 407 ETR's access policy and related procedures (e.g. evacuation)
- specify when the visitation period begins and ends
- specify the purpose of their visit
- greet visitors and sign them into the Entry Log Book or provide the escort's name and contact information if the host will not be escorting the visitor

Escorts must:

- greet visitors, and sign them into the Entry Log Book
- inform visitors about 407 ETR's access policy and related procedures (e.g. evacuation)
- accompany visitors while they are in non-public areas, or transfer responsibility to another escort
- ensure visitors exit the premises securely
- ensure visitors return their visitor's badge to the Security Desk

Visitors must:

- comply with all 407 ETR's corporate policies/procedures as provided to them
- sign in at the security desk
- display their visitor's badge prominently
- identify themselves, their purpose, host, and escort in response to any question

The Security Officer must:

- ensure the host has provided visitors' information,
- contact the host and/or escort once the visitor has arrived
- ensure the badge is returned when the visitor is leaving

Entry and Access Logs

Access to 407 ETR Premises

407 ETR requires that an Visitor Log be completed for any visitors to 407 ETR; the Visitor Log should capture the information listed below:

Visitor name	Host name	Badge number
Company (if applicable)	Entry and exit times	Date of visit
Purpose of visit	Badge returned by visitor	

- Visitors will be asked to review the Physical Access Policy prior to entering the premises.
- 407 ETR's Security Desk will store the Entry Log in a secure location for 3 months.

Access to Sensitive Areas

407 ETR requires that a log be created for each person when they enter and exit a sensitive area (visitors and employees alike.) Access to sensitive areas such as computer or server rooms is limited to specific individuals and controlled through their access badge. The access system creates and retains a record of individuals who enter and exit. If required a system log can be requested from the Security Desk that will provide the details of who has accessed a sensitive area in addition to the time.

Visitor Access Guidelines

Visitor access to premises and property is based on the description provided below.

Area	Access Description
Public areas	Free access
Washrooms	Accompany to and from the washroom area
Common areas	Accompany to and within common areas
Meeting rooms	Accompany to and within meeting rooms.
Sensitive areas	Requires elevated access, authorized by the area Manager, visitors must be accompanied to, from, and within sensitive areas. Sensitive areas contain card data and other like data or records. A card access record that identifies anyone entering the areas listed below, must be generated and maintained: • server room or computer rooms • telephony room
Controlled Areas	Requires special access, authorized by the area Manager, visitors must be accompanied to, from, and within controlled areas. Controlled areas include: • Cash Administration • Mail Room • Transponder Room • Vault Room
Patrol Yard	Accompany to and from patrol yard and applicable buildings

Visitor access to 407 ETR services/assets is based on the description provided below.

Service	Access Description
Telephones	Dialing from escort`s desks allowed according to escort`s dialing privileges.
Photocopiers	Copies/printing assisted by escort
FAX machines	Faxing assisted by escort
Computers	Access to a 407 ETR computer only if purpose of visit is to provide technical support to 407 ETR's computers. Entrance to computer rooms is monitored through the use of CCTV. Escort must supervise all access directly.

Network	Wireless access is separated into two networks public and corporate, The corporate access will be secured by firewall policies. Access to guest wired jacks in public areas and meeting rooms allowed. Access to guest wireless network allowed using weekly wireless password provided by IT to the escort or host.

CCTV and Video Surveillance

Surveillance cameras have been installed to assist in safeguarding 407 ETR employees, assets, and property. Building entrances, hallways, doors to sensitive and controlled areas are equipped with surveillance cameras in the event there is an incident that requires 407 ETR to investigate the incident.

Recorded images created by video surveillance and related equipment are stored in a secure location with access limited to Security and Facilities personnel only.

Retention periods for recorded images from CCTV cameras are determined by business requirements and by applicable laws and regulations.

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, Human Resources

Related Policies

030 – Information Systems Security and Use

004 B - CCTV and Video Surveillance Policy

Related Procedures

025 A – Physical Access Procedures

Related Forms

Visitor Logs
Visitor Information Brochure

Related Scripts

N/A

Revision History

Date	Version Number	Modifications
January 20, 2012	1.0	New policy issued.
July 03, 2013	2.0	Non-material changes, added policy links and statement on access to building access system/badges
March 12, 2014	3.0	Annual review completed by HR and BPM, converted to new policy format. No material change to policy content.
August 21, 2015	4.0	Annual review conducted by HR and BPM, no material change to policy.
October 25, 2016	5.0	Annual review conducted by HR and BPM, no material change to policy.
November 25, 2017	6.0	Annual review conducted by HR and BPM, no material change to policy.

Policy Authorization

Policy Approvers	Approval Date
Jose Tamariz President and Chief Executive Officer	January 20, 2012
Louis-M. St-Maurice Chief Financial Officer	January 17, 2012
Wayne Anthony VP, Human Resources	December 29, 2011
Robert Ives Chief Information Officer	December 14, 2011
Randy Luyk VP, BPM	December 07, 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.