SECTION 7 - AIRPORT SECURITY

A. GENERAL

This section includes those non-Sensitive Security Information (SSI) requirements set forth in the Airport Security Program (ASP), issued by the Chief Executive Officer (CEO) under 49 Code of Federal Regulations (CFR) Part 1542 – Airport Security.

The requirements of this section are critical to the safe and secure operation of the Airport, our first priority, and implemented in furtherance of the Airport's responsibility to ensure compliance with airport security regulations required by the laws of the United States and regulations of the Transportation Security Administration (TSA).

For the purpose of this section only, any areas described as Secured Area, Sterile Area, Restricted Area, Security Identification Display Area (SIDA), or Air Operations Area (AOA), whether within a building, terminal, or on the airfield, shall be referred to collectively as the "Restricted Area."

All personnel working and doing business on Airport property must always comply with this section and model the significance of safety and security for co-workers, passengers, and members of the public. No person or vehicle may enter or be present within any Restricted Area unless the entry and presence is performed in accordance with this section and/or the ASP.

All security badgeholders have an affirmative duty to maintain a secure airport. Tenants, contractors, and permittees are responsible for ensuring that their employees, suppliers, contractors, subcontractors, and all other businesses and entities providing services on Airport property comply with these requirements.

Any person who violates a security requirement, compromises Airport Security, or otherwise creates or engages or participates in any unsafe, unsecure, or hazardous condition or activity at the Airport, may have his/her access privileges immediately revoked on a temporary or permanent basis at the sole discretion of the Airport. The offender(s) shall also be responsible for remediation of property damage or personal injury and any resulting cost, including any fine imposed by the Airport and/or regulatory agency.

B. PARTICIPANT

Each air carrier, licensee, tenant, vendor, or contractor requiring Security Badges shall become a "Participant" in the Airport Rules and Regulations, the ASP, and remain in good standing to retain airport privileges.

Any new licensee, vendor, or contractor requesting security badges must be sponsored by an existing Participant. The sponsorship requirement shall establish the licensee, vendor, or contractor has a legitimate operational need for the requested access.

The licensee, vendor, or contractor requiring security badges must obtain an enrollment packet from the Security Badge Office to initiate their company's enrollment process. Enrollment packets, to include: 1) Letter of Intent, 2) Letter of Verification, 3) Letter of Authorization, and 4) Insurance Requirements, and/or other requirements, may be obtained on a walk-in basis at the Security Badge Office, or requested via email, at ontsecuritybadgeoffice@flyontario.com.

A company sponsoring a Participant must immediately notify the Security Badge Office when that sponsorship is terminated.

Each Participant is required to designate an Authorized Signatory to act as the Participant's SAFE Program Coordinator. The Authorized Signatory shall be designated in writing by the Participant.

C. AUTHORIZED SIGNATORY

The Authorized Signatory's primary responsibility is to ensure the Participant's willful and sustained compliance with this section, Appendix 4 – Security Badge Program, Appendix 5 - Security and Airfield Enforcement Program (SAFE), and the specific requirements set forth in the Authorized Signer Manual administered by the Security Badge Office. The Authorized Signatory is the primary point of contact between the Participant, the Security Badge Office, and other Airport Officials, and shall be directly involved with security violation mitigation and associated corrective action efforts.

As directed by the Airport Security Coordinator (ASC) or designee, the Authorized Signatory shall disseminate and effectively implement applicable security measures for the Participant, as adopted and/or revised by the Airport.

The Authorized Signatory is responsible for various security responsibilities, to include the authorization of all employee fingerprinting and badging applications, applicant identity verification, security badge accountability, access changes, security key user agreements, vehicle permits and driving privilege requests.

Unless specifically approved by the ASC or designee, each Participant shall designate a minimum of two (2) Authorized Signatory's, to include one (1) Primary, and one (1) Alternate. The Primary Authorized Signatory shall be the responsive individual for all security badge and/or security key audits performed by the Security Badge Office.

Eligibility

Unless specifically approved by the ASC or designee, and, in coordination with the Security Badge Office, each Authorized Signatory must be a direct employee of the organization; and

1) Designated on a Letter of Authorization (LOA) from the highest-ranking local

official of the organization. If the Authorized Signatory changes, a new LOA must be immediately provided to the Security Badge Office; and

2) Pass a Security Threat Assessment (STA) and Criminal History Records Check (CHRC). Participant's designating the Authorized Signatory are not required to complete an STA or CHRC if they do not have the authority to request a security badge on behalf of their employees, or otherwise do not require a security badge; and

3) Maintain an active security badge; and

4) Complete Authorized Signatory Training and Annual Recurrent Training for the access-controlled area for which applicants shall be sponsored to receive a security badge. For example, an Authorized Signatory only sponsoring applicants for a sterile area security badge will only be required to complete sterile area training; and

5) Submit and maintain an active Authorized Signatory Designation Form.

Primary Responsibilities

Each Authorized Signatory is required to effectively implement the following security requirements as they apply to the Participant; failure to follow these requirements may result in revocation of Authorized Signatory privileges and/or suspension or revocation of the Authorized Signatory's security badge.

1) Airport Rules and Regulations
2) Sponsorship Requirements
3) Authorized Signatory Manual
4) CHRC and STA Background Check Procedures
5) Security Badge Training
6) Escort Procedures and Training
7) Vehicle Search Procedures and Training
8) Motor Vehicle Operating Permit (MVOP) Procedures
9) Driver's Training and Permit Procedures
10) Security Key / Access Code / Security Badge Issuance, Accountability, and Audit Procedures
11) Security Badge and Key Termination and Recovery Plan
12) Security and Airfield Enforcement Program (SAFE)
13) Stop List Procedures

Additionally, each Authorized Signatory is required to perform the following:

1) Promptly notifying the highest-ranking local official when removed as an Authorized Signatory and ensuring the required documents have been

submitted and received by the Security Badge Office; and

2) Maintain required records in accordance with Security Badge Office policies and procedures; and

3) Actively review information and keep abreast of changes in the Security Badging Program; and

4) Provide the Security Badge Office with written notice of any changes to the Participant's contact information, or changes impacting the information reflected on security badges, to include mergers, corporate name changes and entity separations; and

5) Provide immediate notification to the Security Badge Office when there is reason to believe an applicant or current security badgeholder poses a security threat or does not have lawful presence in the United States.

D. PROTECTION OF SENSITIVE SECURITY INFORMATION (SSI)

Sensitive Security Information (SSI) is information that, if publicly released, would be detrimental to transportation security, as defined by 49 CFR. Parts 15 and 1520.

Any person creating or receiving SSI in order to carry out airport security responsibilities is considered a "covered person" under the SSI regulations and has a special obligation to protect this information from unauthorized disclosure pursuant with 49 CFR. Parts 15 and 1520, to include not divulging any security source documents or information (SSI) to any individual, unless the individual has a specific and valid need to know such information.

In addition to 49 CFR. Parts 15 and 1520, all security badgeholders must comply with the Airport's SSI Control Plan administered by the Airport Security Coordinator.

E. AIRPORT ISSUED SECURITY BADGES

Individuals with unescorted access authority entering a secured area shall, in accordance with this section, display an airport issued and/or airport approved security badge at all times. Individuals with unescorted access authority entering a Passenger Terminal must be in possession of their airport issued and/or approved security badge at all times.

Airport issued security badges are issued in varying access levels based upon operational need. Badge colors indicate general areas of authorization based upon an individual's job function. A badge color does not determine access point privileges; rather, the individual's company, job title, and operational need will determine what access control profile is provided.

Certain badge icons may be affixed to security badges indicating additional authorization in

direct correlation with the employee's job function (e.g., escort privileges, airfield driving privileges, federal inspection services area access).

Unless revoked, suspended, or expired, the following classes of security badges, when properly used or displayed by the person to whom they are issued, are recognized as airport-issued and valid:

Terminal ID

Issued to those persons authorized unescorted access to Passenger Terminals for employment purposes only, but not authorized for unescorted access to the secured area. The Terminal ID is issued only to those persons who have passed TSA-mandated background checks.

Secured Area Badges

Secured area badges are issued to those persons authorized unescorted access to all or part of the secured area. Secured area badges do not authorize airfield driving privileges and are issued only to those persons who have passed TSA-mandated background checks.

F. AIRPORT APPROVED SECURITY BADGES

In addition to a valid airport-issued security badge issued by the Security Badge Office, the following unexpired security badges and credentials, when used and/or displayed by the person to whom they are issued, are recognized as airport-approved and valid:

1. Aircraft Operator Security Badges – Flight Crew, Cabin Crew and Mechanics

   Security badges issued and controlled by Aircraft Operators pursuant with their TSA approved Airport Operator Standard Security Program (AOSSP) and 49 CFR Part 1544, or Model Security Program (MSP) and 49 CFR Part 1546.

   Passenger Terminals: Airline identification badges issued to flight crew, cabin crew members, and transient aircraft mechanic personnel not based at ONT, authorize unescorted access to the Passenger Terminals; and authorize unescorted movement in the following portions of the secured area:

   - The immediate vicinity of the aircraft to which the flight crews and cabin crew are assigned;
   - Flight crew and cabin crews operations/flight office or the equivalent;
   - Those areas of a secured area between the areas described above.

   Flight crew and cabin crew members must be in uniform and display their airline-issued

identification on the outermost garment, at waist level or above.

2. FAA Form 110A

   FAA Form 110A - Aviation Safety Federal Credential is recognized as authorizing FAA Aviation Safety Inspectors unescorted access to a Restricted Area when conducting official business.

3. FAA/TSA Credentials

   FAA Agents and TSA Officials in possession of their respective federal credentials, to include TSA Inspectors, Federal Security Directors, Deputy Federal Security Directors, and Assistant Federal Security Directors, are approved for unescorted presence in Restricted Areas when conducting official business.

4. FBI Special Agents / Federal Law Enforcement Officers

   Federal Bureau of Investigations Special Agents and federal law enforcement officers with official credentials, issued by the respective federal agency, are approved for unescorted access to Restricted Areas when conducting official business.

5. Other Approved Security Badges

   Other security badges may be temporarily approved by the ASC. The acceptance of other security badges or identification media by the Airport does not give the bearer(s) permission to be in any part of a Restricted Area unless access is for official business.

G. RESPONSIBILITIES OF SECURITY BADGEHOLDERS AND OTHER PERSONS

1. Transportation Security Regulations

   All persons in possession of a security badge, applying for a security badge, and those with authority to authorize the application or possession of a security badge for use at the airport, must comply with applicable provisions of 49 Code of Federal Regulations (CFR) Parts 1500-1699, which may be obtained through the ASC, or accessed online at Electronic Code of Federal Regulations (e-CFR), at https://ecfr.io/Title-49/chapterXII.

   Security Responsibilities of employees and other persons while employed or conducting business at the Airport, require that no person may:

   - Tamper or interfere with, compromise, modify, or attempt to circumvent any security system, measure, or procedure implemented under the ASP and TSA Regulations; or

- Enter or be present within a Restricted Area without complying with the systems, measures, or procedures being applied to control access, as defined in the ASP; or

- Use or allow to be used any airport-issued access medium or identification system that authorizes the access, presence, or movement of persons or vehicles in a Restricted Area in any unauthorized manner.

Civil Penalties Imposed by Transportation Security Administration (TSA)

Any Participant shall be responsible for payment or reimbursement to the Airport for any civil penalties imposed by the TSA for individual security violations by their employees for violations under Title 49 CFR Part 1542. An employee may be personally subject to civil penalties imposed by the TSA for individual security violations they commit under Title 49 CFR Part 1542.

TSA Investigations

If ONT is made aware a security badge holder is under investigation by the TSA for an individual security violation(s), the security badge may be suspended until such time the Security Badge Office is provided with formal documentation from TSA advising the investigation is complete and resolved.

2. Official Business Only

Security badge holders are strictly prohibited from accessing any Restricted Area of the airport unless the access, to include the escorting of any individual, is performed in accordance with official duties of the Participant, or, for non-business purposes, with prior written approval from the Participant and the ASC or designee. Security badge holders accessing any Restricted Area for non-business purposes without such approval, are subject to immediate suspension and/or revocation of access privileges.

3. Airport Approved Non-Business Purpose – Passenger Terminal Access Only

Security badge holders approved by the Participant and the ASC or designee to access a passenger terminal of the airport for non-business purposes must: 1). Enter using the TSA Checkpoint, 2). Present their person and accessible property for TSA screening, 3). Not access areas of the airport otherwise inaccessible to the public, and 4). Not use their security badge for access purposes. The security badge may only be used for identification and verification purposes at the TSA Checkpoint. Security badge holders failing to enter the passenger terminal using the TSA

Checkpoint for non-business purposes are subject to immediate suspension and/or revocation of access privileges.

4. Security Badge Use and Display

Each unescorted person within a Security Identification Display Area (SIDA) must continuously display their unexpired airport-issued or airport-approved security badge on their outermost garment and above waist level. Any person within a SIDA without a security badge must be escorted as described in this section and the ASP.

5. Duty to Challenge

Any individual issued a security badge has the responsibility to challenge unescorted individuals not clearly displaying a security badge within a secured area and/or other area designated a SIDA.

Badged personnel must conscientiously observe for the presence of a security badge on other employees. Persons performing a security badge challenge must approach and require the person they are challenging to present their security badge. If a security badge is presented, the challenger will ensure:

(1) Badge is valid for area of use;

(2) Badge has not expired;

(3) Photograph on badge matches person holding badge; and

(4) As to any individual failing to produce a security badge or is not under proper escort, badged personnel shall immediately contact and provide a detailed description to the Ontario Police Dispatch at 909-986-6711, or call 911. Badged personnel must not attempt to physically restrain any individual; they must make every effort to keep such individual under visual observation until Airport Officials/Law Enforcement personnel arrive.

If the challenger has reason to fear for their personal safety, or otherwise uncomfortable with performing a direct challenge of unbadged individuals (i.e. requesting security badge), the duty to immediately report the incident to the Ontario Police Dispatch and to make every effort to keep such individual under visual observation until Airport Officials/Law Enforcement personnel arrive remains.

6. Escorting

   All escorting must follow TSA Regulations, which mandates strict control over anyone being escorted into and within a Restricted Area. It is the responsibility of the badged employee acting as the escort to ensure all rules are followed. Failure to do so may result in loss of escorting privileges for two (2) years and possibly other penalties.

   Escorting is only authorized by Airport-issued security badge holders with escort privileges; who may only escort in those areas authorized by his or her access control profile and must keep individuals under his or her escort, in view and under control at all times.

   Escorting of Employees and Security Badge Applicants: The maximum number of days an airport tenant employee or potential employee may be escorted before the individual must apply for a security badge is ten (10) business days. Until such time the security badge application process is complete, individuals who have applied for a security badge must have an identification access control receipt provided by the Security Badge Office in their possession while being escorted within the secured or sterile areas.

   Escorting of Individual or Group: The person(s) being escorted must have a valid government-issued photo identification in their possession. Preferably, no more than three (3) persons may be escorted by one badged individual; up to five (5) is allowed under certain circumstances, as long as control is assured. Requests to escort more than five (5) people must have approval from the ASC or designee.

7. Security Badge Holders with Multiple Employers

   Security badge holders employed by multiple employers must use and display the proper company security badge when representing each company. The security badge is not interchangeable.

8. Unauthorized Use of Security Badge

   It is strictly prohibited to lend or share a security badge, or to use a security badge by anyone other than the person originally issued the security badge.

9. TSA Security Screening/Bypassing

   When traveling as a passenger, or when the intent is to travel as a passenger during off-hours or upon completion of airport work, a security badge holder must enter the Passenger Terminal through a TSA Screening Checkpoint or TSA approved process

(including Known Crew Member doors for eligible flight crew members) with any accessible property intended to be carried onboard an aircraft. The screened security badge holder must remain in the Passenger Terminal. If a screened security badge holder exits the Passenger Terminal, they must exit the Passenger Terminal with any accessible property intended to be carried onboard the aircraft and be re-screened at a TSA Screening Checkpoint. Any attempt to enter the Passenger Terminal with accessible property through an airport-controlled portal will be considered bypassing the screening process and result in the immediate confiscation of the individual's security badge.

10. Badge Holders on Long Term Leave

Every badged individual engaging a leave of absence for thirty (30) consecutive days or more shall surrender his/her security badge and security keys to their Authorized Signatory. This requirement applies to every type of leave, including, but not limited to, medical leave, workers' compensation leave, leave under the Family Medical Leave Act, military leave, jury duty, temporary furlough, compensatory time off, and vacation.

Duty of Authorized Signatories: Authorized signatories shall collect and secure all security badges and security keys before badged individuals commence extended leaves of absence. Airport security badges and security keys shall be provided to the Security Badge Office within two (2) calendar days of leave commencement. Authorized Signatories shall also submit an Employee Extended Leave form to the Security Badge Office.

Leaves of Uncertain Duration: Where a badged individual commences a leave of fewer than thirty (30) consecutive calendar days and the leave is extended beyond thirty (30) consecutive calendar days, the Authorized Signatory shall notify the Security Badge Office by the 30th day that a leave has been extended and shall complete the Badge holder Extended Leave form within three (3) calendar days. The Security Badge Office shall immediately suspend security access, and the Authorized Signatory shall return Airport property (security badge, keys) to the Security Badge Office within two (2) calendar days of such notification.

Re-entry Following Extended Leave: When a security badge holder returns to work from an extended leave, the Authorized Signatory shall contact the Security Badge Office to reactivate the individual's security badge and advise when the individual will retrieve the badge and keys (if applicable). In the event a badge has expired while an individual is on leave, or in cases where the leave exceeds one-hundred and eighty (180) days, the affected employee must successfully complete 1). a criminal history records check, 2). A security threat assessment administered by the Transportation

Security Administration, and 3). Security training administered by the Security Badge Office.

Every individual who fails to surrender their security badge and keys upon request will be subject to immediate and permanent badge revocation.

11. Subject to Search

All persons, except for Law Enforcement Officers and TSA management and regulatory inspectors, as assigned by the ONT Federal Security Director, are subject to inspection/screening by Airport Officials, Law Enforcement, or TSA, when accessing, or present within Restricted Areas of the Airport.

- The inspection/screening may extend to both the individual and accessible property to determine whether the individual impermissibly possesses any explosive materials or other prohibited item in the Restricted Area.

- All employees with a security badge may be subject to such inspection/screening, and acknowledge that consent to such an inspection/screening is a condition for the Airport to issue a security badge, and agree to submit to and cooperate with such an inspection/screening upon request.

- Failure to submit to, or cooperate, with such an inspection/screening, may result in the immediate suspension and revocation of an individual's security badge. Badged personnel are strictly prohibited from circumventing or avoiding security inspections. Any badged individual who does not submit to an inspection while entering or within a Restricted Area is subject to citation, immediate suspension of his/her security badge, and removal from the Restricted Area.

12. Unauthorized Individuals and Vehicles

Unidentified or unauthorized personnel and/or vehicles in the Restricted Area may be removed by Airport Officials at the owner's expense.

13. Unauthorized Use or Duplication of Security Keys

It is strictly prohibited to duplicate or allow the duplication of a security key; or to lend or share a security key, or to use a security key by anyone other than the person originally issued the security key.

14. Unauthorized Use of Security Codes

    It is strictly prohibited to lend or share a security code, or to use a security code by anyone other than the person issued the security code.

15. Security Violation Enforcement

    As further described in the Security and Airfield Enforcement (SAFE) Program (Appendix 4), Airport Officials conduct daily inspections, tests, respond to airport incidents, and enforce identified violations.

    All permittees and security badge-holders are subject to enforcement action when reasonable grounds exist to believe that a violation has occurred, either by commission or omission, of the following: 1). All Security Violations; 2). All Motor Vehicle and Pedestrian Safety Violations involving ground movement and the safety of personnel, aircraft, vehicles, aircraft fueling, and fuel storage/handling occurring within the Airport Operations Area (AOA); and 3). All Landside and/or Ground Transportation violations involving commercial vehicle operators, owners, and drivers transporting or offering to transport passengers, pursuant with the Ground Transportation Rules and Regulations, at flyontario.com.

    The ASC and/or designee reserves the right to deny, suspend, revoke, or limit the scope of an individual's security badge, endorsements or privileges based upon reasonable grounds and giving due consideration to the nature of the offense. No enforcement decision shall establish precedent, and every instance of noncompliance is considered independently.

16. General Security Violation Penalties

    Suspension or Revocation of Access Privileges: Upon either suspension or revocation of a security badge holder's access privileges, the Airport will deactivate and confiscate any security badge issued to the affected security badge holder. The security badge holder must not enter any Airport Restricted Area and must surrender the security badge to the Security Badge Office, the Ontario Police Department, or other requesting Airport Official. Violators may be subject to arrest for criminal trespass (Exception: Individual is in possession of a valid airline ticket with an arrival or departure time scheduled within four (4) hours of Sterile Area entry).

    Suspension or Revocation of Company Access Privileges: Upon either suspension or revocation of an employee's access privileges, the Airport may deactivate and/or confiscate any or all security badges held by the affected employer, including the security badge of all employees, contractors, and agents whose access privileges

were authorized by that employer. All affected employees must immediately surrender any security badge authorized by the employer to the Security Badge Office, the Ontario Police Department, or other Airport Official. If a security badge holder is within a Restricted Area of the Airport, they must immediately depart that area. The Airport may also cancel the affected employer's ability to request the issuance of security badges, unless waived by the ASC.

Reauthorization of Unescorted Access Privileges: In all cases, if a security badge holder's access privileges have been revoked and the ASC has authorized the access privileges to be reinstated, the security badge holder must pay all associated fees, and meet all other re-issuance requirements directed by the Security Badge Office and 49 CFR Part 1542.

Escort Prohibition: It is strictly prohibited for any security badge holder to knowingly escort into a Restricted Area any person whose access privileges have been suspended or revoked, or anyone who has failed the required background checks, a security threat assessment, or criminal history records check.

Applicants with Disqualifying Conviction: Participants must ensure security badge applicants who fail the TSA-mandated fingerprint-based criminal history background check, as described in the Security and Airfield Enforcement Program (Appendix 4), and specified in 49 CFR §1542.209, and/or fail the security threat assessment, are prohibited from accessing a Restricted Area, with or without an escort (Exception: Individual is in possession of a valid airline boarding pass with an arrival or departure time scheduled within four (4) hours of Sterile Area entry).

17. Airport Security Testing

Testing of airport security measures may only be performed by those individuals authorized by 49 CFR §1540.105(b). Upon written request, the ASC may approve testing authorization to tenants or other operators. The request must specify: 1). time period for testing, 2). specific measures to be tested, and 3). testing methodology. All authorized testing must be consistent with airport approved testing methodologies.

Prior to commencing with any ASC approved internal testing, tenants must notify OPD Dispatch at (909) 986-6711. Notice must be given at least two (2) hours prior to testing. OPD Dispatch must be advised of the date and time of the testing period, the location where the testing will take place, the type of test (e.g. badge challenge), and when the testing has been completed.

18. Restricted Area Limitations on Personal Bag Size

All persons issued a security badge and having access to Restricted Areas of the airport, shall have in his/her custody or control no more than two (2) total accessible personal items (bags, purses, backpacks, totes, messenger bags, computer bags, luggage, fanny packs, briefcases, coolers, boxes or any other type of container or combination thereof), unless the bags are: 1). Required for official business purpose; or 2). Required to transport medically necessary items.

Each bag may not be larger than 8”x12”x21”, unless the bag is: 1). Required for official business purpose; or 2). Required to transport medically necessary items. Items not meeting these requirements must be screened as a delivery by Airport Officials or screened at the TSA security checkpoint.

19. Authorization to Enter Airport Restricted Areas

Passenger Terminals

In accordance with this section, the ASP, and applicable federal, state and city laws and regulations, only ticketed passengers, non-traveling persons in possession of an airline-issued or airport-issued authorization, airport-issued security badge holders, escorted individuals, airport-approved security badge holders, and airport-approved credentialled personnel, are authorized by the airport to enter passenger terminals.

Air Operations Area

In accordance with this section, the ASP, and applicable federal, state and city laws and regulations, only airport-issued security badge holders, escorted individuals, airport-approved security badge holders, and airport-approved credentialled personnel, are authorized by the airport to enter the Air Operations Area.

H. GENERAL ACCESS CONTROL REQUIREMENTS AND PROHIBITIONS

Security badge holders must control access to the Restricted Area in accordance with ASP approved procedures implemented to control such access and must engage in the careful use of any door or gate under their control.

1. Access Media

Each security badge holder entering the Restricted Area through any door or gate, must use the security badge, security key, or security code issued specifically to them. Only one (1) security badge holder may access the Restricted Area through

any door or gate at one (1) time.

All security badge holder's and those security badge holders issued a security key are responsible for safeguarding his/her respective security badge and issued security key and for returning both to the Security Badge Office when the operational need is no longer required.

All security badge holders issued a security badge access code or security lock code by the Security Badge Office must ensure the code is kept in his or her immediate control to prevent unauthorized use. The security badge holder shall not write or verbally announce in a public manner the security code(s).

2. Expiration of Operational Need

When a security badge and/or security key is no longer required, to include the expiration of the security badge, the Authorized Signatory must retrieve the security badge and security key and immediately notify the Security Badge Office in person, by phone, or by whatever means possible to ensure that the security badge is immediately deactivated. The Authorized Signatory must deliver the surrendered security badge and/or security key(s) to the Security Badge Office during business hours within two (2) business days of the change in status. A receipt providing proof of the return will be provided upon request. The receipt will provide sufficient proof to avoid any potential penalties for unreturned controlled items. Security badges and security keys may be mailed in, with the understanding that it is the responsibility of the employee and/or company to provide specific proof of return to avoid any associated penalties. Additional security badges or security keys may not be issued to the employer until the security badge or security key is returned.

3. Lost Security Badge or Security Key

If a security badge and/or a security key is lost, the security badge holder must immediately notify the Security Badge Office in person, by phone, or by whatever means possible to ensure that the badge is immediately deactivated. The individual may be subject to a seventy-two (72) hour waiting period for re-issuance, in addition to any monetary fines and fees. All parts and labor costs associated with a lost security key, to include the replacement of locks and associated security equipment, shall be assessed to the employer responsible for the lost security key.

4. Stolen Security Badge or Security Key

When a security badge or security key is reported stolen, the security badge holder

must immediately notify the Security Badge Office by phone to ensure the security badge is immediately deactivated. Replacement badges are issued by the Security Badge Office; the security badge holder must submit a new badge application, provide a police report demonstrating the theft was reported and under investigation, pay all associated fine and fees, and meet all other re-issuance requirements directed by the Security Badge Office and 49 CFR Part 1542. All parts and labor costs associated with a stolen security key, to include the replacement of locks and associated security equipment, shall be assessed to the employer responsible for the lost security key.

5. Receipts for Returned Airport Security Badges and/or Security Keys

The Security Badge Office will provide a receipt when a security badge and/or a security key is returned. Receipts should be retained as proof of the returned item(s).

6. Administrative Fines – Lost Security Badges

Administrative fines are determined by the number of security badges lost by an employee during a rolling two (2) year period beginning with the date of the first reported lost security badge. Fines may be refunded if the lost badge is located within seven (7) calendar days from date of loss. If a badge is located between eight (8) and thirty (30) days, the employee may apply to the ASC or designee to have the fine returned. The ASC may uphold the fine or decide to return all or a portion of the fine, depending on circumstances and the number of occurrences. If two (2) or more security badges are lost, no further badges will be issued for a period of two (2) years. The ASC may deviate from this policy using evidence of extenuating circumstances or other contributing factors.

7. Reporting Subsequent Disqualifying Criminal Convictions

Any individual possessing a security badge must report to his/her supervisor or Authorized Signer within twenty-four (24) hours if he/she has been convicted, given a deferred sentence, found not guilty by reason of insanity, or has been arrested and awaiting judicial proceedings for any felony charge in accordance with 49 CFR 1542.209.

8. Piggybacking

It is strictly prohibited for any individual to follow, allow another to follow, or access a Restricted Area in any way through a controlled access point, unless during authorized escorting. “Piggybacking” occurs when a security badge holder fails to ensure a door or gate closes behind the security badge holder and an unescorted

person gains access to the Restricted Area by bypassing the means to prevent such unauthorized access.

9. Securing Doors and Gates

After each entry and exit, security badge holders must ensure Restricted Area access doors and gates are closed and secured. Before leaving the vicinity of an open Restricted Area Door, to include baggage belt doors and jet-bridge doors, the attending badged personnel shall take deliberate action to ensure the door is properly closed and secured. Under no circumstance should the attending individual leave the immediate vicinity of an open door until it is properly closed and secured.

10. Door Alarms – Duty to Notify

Badged personnel are required to immediately report any self-activation of a door alarm. When an audible alarm sounds at a door the security badge holder has opened, the security badge holder must immediately close and secure the door, contact the Ontario Police Dispatch by phone, and remain at the door until arrival of response personnel.

11. Door Alarms - Duty to Respond

Any security badge holder in the vicinity of an access control point emitting an audible alarm shall assess the immediate area for unauthorized personnel. After completing the assessment, the security badge holder must ensure the door is secured and immediately notify the Ontario Police Dispatch at 909-986-6711, or by dialing 911.

12. Vehicle Gates

Only one vehicle may enter through a vehicle gate unless the security badge holder gaining access is escorting other vehicles. The driver must have a valid security badge indicating they are authorized to access and drive within the Restricted Area. Passengers in the vehicle with a security badge must exit the vehicle and present their security badge for inspection. Passengers in the vehicle without a security badge must present a government-issued photo ID for inspection. The security badge holder entering or exiting the vehicle gate, must ensure the gate is completely closed prior to driving away. If exiting from the secured area with other vehicles, the security badge holder driving the last unescorted vehicle is responsible for ensuring the gate closes and secures before driving away.

General Access Control
Requirements and Prohibitions Continued

13. Vehicle Gates / Pedestrian Prohibition

Authorized security badge holders (pedestrians) may only access Restricted Areas through pedestrian doors and prohibited from accessing Restricted Areas through any vehicle gate without prior authorization from the ASC or designee.

14. Motor Vehicle Operating Permits (MVOP)

All vehicles operating in the AOA, except for vehicles driven solely on Airport property and not required to be licensed by the State of California (e.g., baggage tugs), must display an MVOP which is visible from the exterior of the vehicle.

- MVOP applications must be completed and signed by an Authorized Signatory. The Authorized Signatory certifies by his or her signature that the vehicle for which the permit is requested has the insurance coverage required by the Airport.

- MVOP requests are processed, reviewed, and verified by Airport Officials prior to their issuance.

- An MVOP may not be transferred between vehicles. Lost or stolen MVOP decals must be reported immediately to the Security Badge Office.

15. Use of Airport Federal Inspection Services (FIS) Facilities

All security badge holders within the FIS facilities during international flight processing must have an FIS seal displayed on their security badge or have a pre- approved exception by Customs and Border Protection (CBP) to be in the facility without a seal. All individuals must have a demonstrated, work-related need to be in the FIS facilities.

- No individual shall open an FIS access point door which would provide access out of the FIS Sterile Area during an international flight.

- No FIS doors may be propped open at any time, except for the emergency exit doors entering the international nodes.

- The FIS seal does not authorize escort privileges. Specifically, the escort privileges provided to a security badge holder by the Airport does not extend to the FIS facility. An on-duty CBP Supervisor may authorize an escort if deemed appropriate.

- Any individual who has no badge access to the FIS facilities must be escorted by CBP, or other authorized personnel approved by CBP, always while in the FIS facilities.

- Bag belts may not be used as a means of entering the FIS facilities.

- It is the Participant's responsibility to ensure all employees requiring access to the FIS facilities, or who work international flights, have FIS seals on their badges. All security badge holders requiring an FIS seal must complete the CBP's application process.

16. Damage to Security Systems

    Under no circumstances may an individual engage in defacing, damaging, hacking, or interacting with any Airport Security System in any manner.

17. Forcing Open Security Doors or Gates

    All persons are prohibited from forcing open a door or gate providing access to an airport Restricted Area.

18. Reporting Malfunctions

    Security badge holder's discovering a malfunctioning alarm or locking mechanism must immediately report the malfunction to the Ontario Police Dispatch.

19. Security Keys

    Security keys are strictly controlled by the Security Badge Office. Loss of a security key may result in the re-keying of numerous doors/locks to ensure the sustained security integrity of the airport. Costs for re-keying associated to lost keys shall be billed to responsible party(s).

I. RESTRICTED AREA DRUG AND ALCOHOL PROHIBITION

As provided under FAR Part 91.11, no pilot or other member of the flight crew of an aircraft in operation on the Airport, or any person attending or assisting in any aircraft operation on the Airport, shall be under the influence of intoxicants (alcohol or drugs), nor shall any person under the influence of intoxicants be permitted to board any aircraft, excluding medical patient(s) under care. The ONT CEO or designee has the sole discretion to deny any person violating this Section.

No individual may transport into the Restricted Area any alcohol, or any drug identified by the United States Drug Enforcement Agency (DEA) as a "Schedule I" drug, nor may any individual with a security badge ingest alcohol or a Schedule I drug eight (8) or fewer hours before work or while at work, including breaks. Schedule I drugs include: heroin, LSD, marijuana, ecstasy, methaqualone, and peyote.
See https://www.dea.gov/druginfo/ds.shtml.

No individual may transport into any Restricted Area any of the following substances unless the individual has a prescription: Any drug identified by the DEA as a Schedule II, III, IV, or V drug.

Prescription Drugs: Individuals with a current prescription for Schedule II-V drugs must have in their possession the medication in the original prescription bottle, with a legible label showing the name of the individual.

Working under the Influence: No individual may enter or remain in a Restricted Area if the individual is in any way impaired as a result of ingesting substances referenced in this rule, including prescription drugs.

J. FIREARMS AND EXPLOSIVES

Reference Subsection 6.2 - Handling of Explosives and Other Hazardous Materials.

Possession: No persons, except authorized law enforcement officers, authorized wildlife control personnel, Federal Flight Deck Officers, U.S. Post Office and Customs and Border Protection Officers, members of the armed forces of the United States on official duty, and persons under escort by a City of Ontario Police Officer, may possess any firearms or explosives within an airport Restricted Area without written permission from the CEO or designee.

All persons other than those in the excepted classes shall, while at the Airport, surrender all such objects in their possession to a City of Ontario Police Officer (909) 986-6711. Requests for permission to possess firearms or explosives shall be submitted in writing to the CEO or designee, who has the sole discretion in granting or denying such requests. Failure to comply with this requirement may result in civil and criminal charges.

Storage: Except for firearms and explosives belonging to authorized law enforcement officers, firearms and explosives may not be stored within the secured or sterile area of the airport, unless a TSA or OIAA approved storage and safety plan is on file in the Office of the CEO or designee. Failure to comply with this requirement may result in civil and criminal charges.

All law enforcement officers and Federal Flight Deck Officers (FFDO) accessing the Passenger Terminal must enter through an approved TSA security checkpoint and follow TSA established credential verification and sign-in procedures. Armed, on-duty local and state Law Enforcement Officers on official business may be escorted into the Restricted

Area by a badged OPD Law Enforcement Officer.

K. ARMED GUARDS, ARMORED VEHICLES, ARMED COURIER SERVICES

Tenants using armed guards and/or armored courier services to, for example, transport currency or high value items or to service automated teller machines, must ensure that its service provider complies as follows:

Badge Required: All armed security guards/couriers accessing any area of the Airport – public (non-Restricted) or Restricted – must be in uniform and in possession of a security badge or under proper escort.

Vehicle access: Private armed guards are not permitted on ramps unless specific approval is obtained from the OPD Airport Bureau Supervisor, (909) 986-6711. Armored vehicles entering a Restricted Area for the purpose of picking up or dropping off freight planeside shall enter only through a Vehicle Screening Checkpoint. All drivers must have a non-movement area driving icon displayed on their security badge and must follow all non-movement area driving rules.

Prior to accessing the Restricted Area, armed vehicle drivers must complete the Armored/Courier Vehicle Information Sheet form and provide it to the OPD at the Vehicle Screening Checkpoint. A point of contact with a mobile phone must always be in the vehicle while on the AOA.

- Armed guards are not permitted within the confines of an airplane
- Private guard dogs may not be used in public or common use areas of the airport

Parking: For the International Terminal, armored courier service vehicles must be parked on either end of the terminal roadway. For Terminals 2 or 4, vehicles may be parked anywhere on the curb. Drivers are prohibited from double parking and/or obstructing active passenger loading or offloading areas.

L. PROHIBITED ITEMS

With the exception of Airport Approved Prohibited Items, Security badge holders may not possess or carry items into or within the passenger terminal that are otherwise prohibited by TSA regulation, including through security screening checkpoints. “Prohibited Items” are defined under 49 CFR § 1540.111, and more specifically described on the TSA website, at https://www.tsa.gov/travel/security-screening/whatcanibring/all;

Security badge holders may not possess or carry items into or within any Restricted Area that are listed as hazardous materials on the FAA web site at www.faa.gov, or any other item deemed as contraband by local law enforcement authorities, without an approved demonstrated operational need.

Any badged personnel who discovers or comes into possession of unauthorized and/or uncontrolled Prohibited Item must immediately contact OPD Dispatch at (909) 986-6711 to have an officer respond for proper confiscation, disposal, and investigation. Under no circumstances may hazardous items be disposed of in a trash receptacle.

Airport Approved Prohibited Items

A limited list of items may be considered exceptions if job related. All security badge holders, tenants, or contractors requiring Prohibited Items to perform their job duties, or for their business operations in a Passenger Terminal, including but not limited to knives, tools, and/or or heavy equipment, must coordinate and obtain prior approval from the Security Badge Office for each prohibited item.

Prohibited items must not be left unattended in the passenger terminal unless, as approved by the ASC or designee, the prohibited items are secured and inaccessible to other individuals, to include screened passengers and/or non-security badge holders. The security badge holder, tenant, or contractor shall demonstrate to Airport Officials how Prohibited Items are secured and be responsible for the proper safeguarding and storage of Prohibited Items and tools during operational and non-operational hours.

All Sterile Area Concessionaire tenants shall audit Airport-Approved Prohibited Item inventories in conformance with the most current version of the Training of Security Responsibilities (TSR) titled “Sterile Area Concessionaire Requirements.” Those with a need to know may obtain a copy of this restricted TSR from the Security Badge Office.

M. UNATTENDED BAGGAGE AND ARTICLES

Unattended baggage and/or articles are prohibited in all areas of the Airport and must be reported to OPD Dispatch immediately. If unattended baggage and/or articles are found, they are subject to search and may be confiscated by OPD or TSA personnel and may be destroyed.

N. PASSENGER TERMINAL DELIVERIES

Any merchandise or consumables intended for sale, consumption, and/or use in a Passenger Terminal, whether to be purchased or obtained from a concession tenant, an airline club or lounge, or at a special event, must be inspected by Airport Officials at the respective Passenger Terminal Loading Dock, or by TSA at the Passenger Screening Checkpoint. Using employee bypass doors to transport non-inspected merchandise or consumables into the Passenger Terminal is strictly prohibited.

Inspections may include the person and belongings of any personnel transporting merchandise or consumables into the Passenger Terminal.

Delivery Testing

Delivery and/or badged personnel shall cooperate with official inspections and security testing performed by Airport Officials and/or TSA Inspectors. Any individual refusing to assist with ongoing security inspections or testing in Restricted Areas of the Airport may be subject to citation and suspension of his/her security badge or access privilege.

O. TENANT VIDEO MONITORING AND RECORDING DEVICES

No video monitoring or other recording devices may be installed or removed by any Airport tenant or permittee in or around the Airport premises without prior written authorization from the ASC or designee. To obtain authorization for CCTV camera installation or removal, tenants and permittees must submit an application to the Security Badge Office, specifying the following:

- Field-of View (FOV) screenshots
- Video monitoring/recording device model and specifications
- Recording system and retention time
- Camera layout drawing
- Security infrastructure and plan to prevent unauthorized access

The use of Pan-Tilt-Zoom (PTZ) security cameras by tenants and permittees in any Restricted area is strictly prohibited and no video monitoring and/or recording device may be installed or focused in a manner that depicts/records security checkpoints, or doors that provide access to any area on Airport premises that, in the sole and exclusive discretion of the ASC or designee, is deemed to present a potential risk to Airport security. All subsequent changes or modifications to tenant and permittee video monitoring and/or recording device use must be submitted to Airport Security Coordinator in writing and approved prior to executing modifications.

Remote Viewing and Authorization Access

No video monitoring and/or recording device data may be streamed or otherwise transmitted on a wireless network unless the wireless network is equipped with WPA2 security. Real-time access to all footage must be available to Airport Officials at all times, as designated by the ASC. No tenant or permittee shall release any video monitoring and/or recording device footage from cameras/devices without prior written authorization from the ASC or designee and, if deemed appropriate, the TSA.

Remote access to video monitoring and/or recording devices in secure areas will not be permitted unless explicitly authorized by the ASC. All forms of video footage, whether real-time or stored, must be password protected. Passwords must comply with the Airport's Password policy.

Inventory of Video Monitoring and Other Recording Devices

All tenants and permittees shall provide ASC with an inventory of existing video monitoring and/or recording devices and security plans, including all of the following:

- Device manufacturer, model and specifications
- Field-of-view
- Data retention time
- Placement of video monitoring and/or recording devices
- Remote access usage
- Written security plan detailing how unauthorized access will be prevented

P. RESTRICTED AREA PHOTOGRAPHY

Still or moving photography undertaken by anyone that may reveal the operation or location of access control readers, security measures or secured doors within or leading into or out of Restricted Areas is prohibited.

Q. RESTRICTED AREA CLEAR ZONE

The Airport Perimeter Fence Area shall remain free of vehicles, stored materials, unattended equipment, or other property. The Airport CEO or his/her authorized representative, may remove, or cause to remove, any unidentified or unauthorized vehicle, or other property, parked in posted “no parking” zones along the perimeter fence ten (10) foot clear zone. Clear Zones may be expanded at the discretion of the CEO or his/her authorized representative, as necessary.

R. PERIMETER FACILITIES

Tenants operating from perimeter-based facilities with direct access to the Restricted Area, must abide by all pertinent rules of operation as applicable to the secured area found in 49 CFR Parts 1540-1548. Inspections and audits by the TSA and/or Airport may be conducted on a regular basis. Any deficiencies will be addressed, and associated fines may be assessed.

Tenants are responsible for controlling access to the Restricted Area from the facilities that they occupy, in accordance with security measures implemented by the Airport. This includes areas that are contracted or subcontracted. Any and all parties with a documented interest in a specific area are responsible.

Tenants, subtenants, lessees, permittees, and/or operators are responsible to ensure compliance with all security measures.

Any TSA fines and/or penalties assessed against the Airport for non-compliance with the ASP and/or Transportation Security Regulations (49 CFR Parts 1500-1699) and arising

from the actions of any entity leasing, occupying or using space (including all tenants, subtenants, permittees, licensees, service providers, invitees and/or operators) anywhere in the Airport, will be passed through to the entity, tenant subtenant, lessee, permittee, service provider, individual and/or operator named as the source of the violation and respective TSA fine.

S. GENERAL NOTIFICATION REQUIREMENTS

Immediate notification to the Security Badge Office from a Participant is required whenever a Participant or Authorized Signer becomes aware of any of the following:

- A security badge or security key is lost or stolen
- A security badge holder's employment status changes through termination, retirement, leave greater than 30 days, or any other form of separation from the company
- An employee may be considered a threat to airport security for any reason
- An employee who has a security badge and/or security key is arrested or convicted of a Disqualifying Crime pursuant with 49 CFR §1542.209

The Participant or the Authorized Signer must contact the Security Badge Office to verbally request immediate deactivation of the security badge – as applicable. If the Security Badge Office is closed, or otherwise unavailable, the employer or the Authorized Signer must contact the City of Ontario Police Dispatch to verbally request immediate deactivation of the Security Badge.