SECTION 7 – Airport Security

LIST OF REVISIONS

The following list identifies all changes and revisions made to this specific Section of the ONT Rules and Regulations Manual.

Date of Revision	Section	Pages	Subject
November 2023	ALL	ALL	Reformatting & Technical Changes
November 2023	D	5	Airport Approved Security Badges
November 2023	D.4	5	Aircraft Operator and Foreign Carrier ID Media
November 2023	E.6(e)	8	Escorting new Employee
November 2023	F.2	12	Subject to Search
November 2023	G	15	ONT+ Visitor Pass Program
November 2023	L	20	Tenant Video Monitoring and Recording Devices
July 2024	ALL	ALL	Reformatting & Technical Changes, consolidated Participant & Authorized Signer information with Appendix IV
May 2025	7.5	7	Escorting New Employee
May 2025	7.7	16	ONT+ Visitor Pass Program

Table of Contents

Page is Intentionally Left Blank

Section 7– Airport Security

7.1 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."

7.1.1 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.

7.1.2 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.

7.1.3 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.

7.2 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.

7.2.1 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.

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

7.3 Airport Issued Security Badges

Individuals with unescorted access authority entering a secured area shall, in accordance with this section, display an airport-issued 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 or airport-approved security badge at all times

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:

7.3.1 Passenger Terminal ID:

Passenger Terminal ID’s are issued to persons authorized unescorted access to a passenger terminal for employment purposes only but are not authorized for unescorted access to the secured area. The passenger terminal ID is only issued to persons who have passed TSA-mandated background checks (Reference Appendix IV).

7.3.2 Secured Area Badge:

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

7.4 Airport Approved ID Media & Credentials

The unexpired ID media and credentials described below, when used and/or displayed by the person to whom they are issued, are recognized as airport-approved and valid for varying and limited unescorted access pursuant with the Airport Security Program.

Individuals in possession of an airport-approved ID media or credential may only access a secured area of the airport after verification of the ID media and/or credential and operational need from one of the following security badgeholders: airport official or authorized representative, a direct employee or authorized representative of an ONT-based Part 1544 Aircraft Operator, or direct employee or authorized representative of an ONT-based Part 1546 Foreign Air-Carrier.

Security badgeholder privileges, including escort or driving privileges, are not extended to airport-approved ID media or credentials.

7.4.1 Aircraft Operator and Foreign Air Carrier ID Media:

7.4.1.1 ID media issued to pilots, flight attendants, loadmasters, flight engineers, and flight navigators assigned to perform duties on board an aircraft during flight time by an aircraft operator regulated under 49 CFR Part 1544 or foreign air carrier regulated under 49 CFR Part 1546, are authorized varying and strictly limited access to the secured area and sterile area pursuant with the Airport Security Program.

7.4.1.2 ID media issued to transient aircraft mechanics (i.e., not based at ONT) assigned to perform official duties for an ONT-based aircraft operator regulated under 49 CFR part 1544, are authorized strictly limited access to the secured area and sterile area pursuant with the Airport Security Program.

7.4.1.3 While within the secured area, the airport-approved ID media must be displayed on the outermost garment, above the waist and below the neck, so as to be readily visible.

7.4.2 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.

7.4.3 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.

7.4.4 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.

7.4.5 Other Approved ID media

Other ID media may be temporarily approved by the CEO or designee. 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.

7.5 General Security Badgeholder Responsibilities

7.5.1 Official Business Only

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

7.5.2 Unauthorized Use of Security Badge, Security Key or Security Code

7.5.2.1 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.

7.5.2.2 Security Key: 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.

7.5.2.3 Security Code: 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.

7.5.3 Security Badge Display

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

7.5.4 Security Badgeholders with Multiple Employers

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

7.5.5 Duty to Challenge

7.5.5.1 Security badgeholders have the responsibility to challenge unescorted individuals not clearly displaying a security badge within a secured area and/or other area designated a SIDA.

7.5.5.2 Security badgeholders 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:

a) Security badge is valid for area of use;
b) Security badge has not expired;
c) Photograph on the security badge matches person holding badge; and
d) An individual failing to produce a security badge or is not under proper escort, the security badgeholder shall immediately contact and provide a detailed description to the Ontario Police Dispatch at 909-986-3371 or call 911. The security badgeholder must not attempt to physically restrain any individual but make every effort to keep such individual under visual observation until law enforcement personnel arrive.

7.5.5.3 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 law enforcement personnel arrive remains.

7.5.6 Escorting

7.5.6.1 Escorting is only authorized by trained airport-issued security badgeholders with escort privileges.

7.5.6.2 All escorting must follow TSA regulations, which require strict control over anyone being escorted into and within a Restricted Area. It is the responsibility of the escort to ensure all rules are followed. Failure to do so may result in revocation of escort privileges for two (2) years and other penalties.

7.5.6.3 Escorts may only escort in those areas authorized by the security badgeholders level of access.

7.5.6.4 Escorted Visitors ID: All escorted visitors must have a valid government-issued photo identification in their possession at all times (e.g., Driver's License).

7.5.6.5 Escorting New Employee: The maximum number of days a new (or potentially new) tenant employee may be escorted within the SIDA, until the new employee is required to apply for a security badge, is ten (10) business days from the first escort occurrence. Until such time the security badge application process is complete, the new employee (security badge applicant) must have a security badge application receipt in their possession at all times while under escort within the SIDA and provide the receipt to any airport official upon request. For those Airport tenants operating within a sterile area concourse, the airport tenant must obtain specific authorization from the Security & Badging Office to escort individuals working within the sterile area.

7.5.6.6 Escorting Group: To ensure strict control, no more than three (3) visitors should be escorted by any one escort, with a maximum of five (5) visitors allowed under certain circumstances. Escorting more than five (5) visitors must be pre-approved by the CEO or designee.

7.5.7 Airport Security Testing

7.5.7.1 Testing of airport security measures is strictly prohibited without specific approval from the CEO or designee. Upon written request, the CEO or designee may approve testing authorization for an aircraft operator or foreign carrier pursuant with 49 CFR §1540.105(b)(2). The request must specify: 1). date, time, and location of testing, 2). specific measures to be tested, and 3). testing methodology. All authorized testing must be consistent with airport approved testing methodologies.

7.5.7.2 Security badgeholders shall fully cooperate with Airport Officials and TSA Transportation Security Inspectors performing official inspections and testing of security badgeholder responsibilities.

7.5.8 Security Violation Enforcement

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

7.5.8.2 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:

a) All Security Violations;
b) 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
c) 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.

7.5.8.3 The CEO 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.

7.5.8.4 Suspension or Revocation of Access Privileges: Upon either suspension or revocation of a security badgeholder's access privileges, the Airport will deactivate and confiscate any security badge issued to the affected security badgeholder. The security badgeholder must not enter any Airport Restricted Area and must surrender the security badge to the Security and Badging 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). It is strictly prohibited for any security badgeholder to knowingly escort into a Restricted Area any person whose access privileges have been suspended or revoked, or failed the required background checks, a security threat assessment, or criminal history records check.

7.5.8.5 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 privilege were authorized by that employer. All affected employees must immediately surrender any security badge authorized by the employer to the Security and Badging Office, the Ontario Police Department, or other Airport Official. If a security badgeholder 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 CEO or designee.

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

7.5.8.7 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 IV), 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).

7.5.9 Transportation Security Regulations

As defined by 49 Code of Federal Regulations (CFR) §1500.3, all persons (e.g., any individual, corporation, company, association, firm, or governmental authority) must comply with applicable provisions of 49 CFR Parts 1500-1699 while at the Airport. All TSA regulations are made available online at www.ecfr.gov.

7.5.10 49 CFR § 1540.105(a)(1)-(3) Security Responsibilities of Employees and other Persons, provides: (a) No person may:

7.5.10.1 Tamper or interfere with, compromise, modify, attempt to circumvent, or cause a person to tamper or interfere with, compromise, modify, or attempt to circumvent any security system, measure, or procedure implemented under this subchapter; and

7.5.10.2 Enter, or be present within, a secured area, AOA, SIDA, or sterile area without complying with the systems, measures, or procedures being applied to control access to, or the presence or movement in, such areas; and

7.5.10.3 Use, allow to be used, or cause to be used, any airport-issued or airport approved access medium or identification medium that authorizes the access, presence, or movement of persons or vehicles in secured areas, AOA's, or SIDA's in any other manner than that for which it was issued by the appropriate authority under this subchapter.

7.5.11 Civil Penalties Imposed by the Transportation Security Administration (TSA)

Participants are 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 – Airport Security. 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.

7.5.12 TSA Investigations

A security badgeholder under investigation by the TSA for an individual security violation(s), the security badge may be suspended until such time the Security and Badging Office is provided with formal documentation from TSA advising the investigation is complete and resolved.

7.6 General Access Control Requirements and Prohibitions

7.6.1 Authorization to Enter Airport Restricted Areas

7.6.1.1 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 gate pass, non-traveling persons in possession of an airport-issued ONT+ visitor pass, security badgeholders, escorted individuals, airport-approved ID media holders or credentialed personnel, are authorized by the airport to enter passenger terminals.

7.6.1.2 Air Operations Area

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

7.6.2 Subject to Search

By order of the Department of Homeland Security (DHS) Transportation Security Administration (TSA), when entering secured area or sterile areas of the airport, all individuals, to include aviation workers (badgeholders) and escorted visitors (non-badgeholders) and their accessible property, are subject to screening by Airport and/or TSA officials for unauthorized weapons, explosives, and incendiaries (limited exceptions). All individuals consent to such screening as a condition for security badge issuance or escorted visit and agree to submit to/and cooperate with such screening upon request. Failing to cooperate and submit to such screening or engaging in any attempt to circumvent or avoid such screening, may result in removal from the secured area or sterile area, immediate suspension or permanent revocation of security badge, airport administrative fine, and other penalty described by applicable local, state, or federal law.

7.6.3 Access Media

7.6.3.1 Each security badgeholder 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 badgeholder may access the Restricted Area through any door or gate at one (1) time.

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

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

7.6.4 Piggybacking

It is strictly prohibited for any individual to follow, or allow another individual to follow, a security badgeholder through a controlled access point, unless the activity is performed during authorized escorting activity. “Piggybacking” occurs when a security badgeholder fails to ensure a door or gate closes them and an individual gains unauthorized access to a Restricted Area by bypassing the means to prevent such access.

7.6.5 TSA Security Screening/Bypassing

7.6.5.1 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 badgeholder 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 badgeholder must remain in the Passenger Terminal.

7.6.5.2 If a screened security badgeholder 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.

7.6.6 Securing Doors and Gates

After each entry and exit, security badgeholders 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 security badgeholder shall take deliberate action to ensure the door is properly closed and secured. Under no circumstance should the attending security badgeholder leave the immediate vicinity of an open door until it is properly closed and secured.

7.6.7 Door Alarms – Duty to Notify

Security badgeholders are required to immediately report any self-activation of a door alarm. When an audible alarm sounds at a door the security badgeholder has opened, the security badgeholder must immediately close and secure the door, immediately contact the Ontario Police Dispatch at 909-986-6711, and remain at the door until arrival of response personnel.

7.6.8 Door Alarms - Duty to Respond

Any security badgeholder in the vicinity of an access control point emitting an audible alarm shall assess the immediate area for unauthorized personnel, ensure the door is secured, and immediately notify the Ontario Police Dispatch at 909-986-6711.

7.6.9 Vehicle Gates

Only one vehicle may enter through a vehicle gate unless the security badgeholder 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 badgeholder 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 badgeholder driving the last unescorted vehicle is responsible for ensuring the gate closes and secures before driving away

7.6.10 Vehicle Gates / Pedestrian Prohibition

Security badgeholders are strictly prohibited from walking through a vehicle gate to access Restricted Areas without prior authorization from the CEO or designee.

7.6.11 Motor Vehicle Operating Permits (MVOP)

7.6.11.1 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.

7.6.11.2 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.

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

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

7.6.12 Use of Airport Federal Inspection Services (FIS) Facilities

7.6.12.1 All security badgeholders 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.

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

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

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

d) Any individual without security badge access to the FIS facilities must be escorted by CBP, or other authorized personnel approved by CBP, while within the FIS facilities.

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

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

7.6.13 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.

7.6.14 Forcing Open Security Doors or Gates

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

7.6.15 Reporting Malfunctions

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

7.6.16 Security Keys

Security keys are strictly controlled by the Security and Badging 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).

7.7 ONT+ Visitor Pass Program

7.7.1 Purpose

The ONT+ visitor pass program is a privilege made available to the non-traveling public at www.flyontario.com/ontplus that provides airport-issued authorizations to access the sterile area concourse for non-travelling visitors.

7.7.2 TSA Screening Checkpoint Requirements

7.7.2.1 Approved ONT+ visitor pass recipients must perform the following:

a) Present their ONT+ visitor pass and government-issued photo ID at the TSA Screening Checkpoint; and

b) Submit to screening of their person and accessible property at the TSA screening checkpoint prior to accessing the sterile area.

7.7.3 Program Restrictions & Prohibitions

7.7.3.1 The ONT+ visitor pass is non-transferrable and valid only on the date of issuance and approved start time.

7.7.3.2 Visitors are subject to the same security regulations as passengers boarding an aircraft and must comply with all TSA's screening procedures, including TSA prohibited item restrictions.

7.7.3.3 In response to exigent circumstances or airport operational needs, the CEO or designee reserves the right to cancel the program, cancel approved ONT+ visitor passes, or modify program rules at any time without prior notice.

7.7.3.4 The ONT+ visitor pass program is specifically for non-traveling individuals – no exceptions. Individuals scheduled or ticketed to depart the Ontario International Airport on a scheduled flight are specifically prohibited from obtaining an ONT+ visitor pass the same day as the scheduled flight

7.7.3.5 The ONT+ visitor pass program only extends to individuals not subject to TSA or airport badging requirements. Unless specifically approved by the Security & Badging Office, individuals working in the sterile area, to include new tenant employees and/or badge applicants, are strictly prohibited from using the ONT+ visitor pass program to access the sterile area concourse.

7.7.4 Security Badgeholder Use

7.7.4.1 Security badgeholders must be off duty. When using an ONT+ visitor pass to access the passenger terminal for non-business purposes, security badgeholders must:

a) Enter using the TSA Checkpoint

b) Present their person and accessible property for TSA screening

c) Not access areas of the airport otherwise inaccessible to the public

d) Not use their security badge for access purposes.

7.7.4.2 Security badgeholders using their security badge for any non-business purpose are subject to the immediate suspension and/or revocation of their security badge.

7.7.5 ONT+ Visitor Pass Program Violations

The ONT+ Visitor Pass Program was implemented in accordance with 49 Code of Federal Regulation (CFR) Part 1560 – Secure Flight Program, §1560.111(a), which applies to a covered airport operator that has a program approved by TSA through which the covered airport operator may authorize non-traveling individuals to enter a sterile area. Failure to comply with this section may represent a violation of 49 CFR § 1540.105(a)(2) - Security Responsibilities of Employees and other Persons, which prohibits any person from entering, or being present within, a sterile area without complying with the systems, measures, or procedures being applied to control access to, or the presence or movement in, such area.

7.8 Restricted Area Drug and Alcohol Prohibition

7.8.1 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 CEO or designee has the sole discretion to deny any person violating this Section.

7.8.2 No individual may transport into a Restricted Area any alcohol, or any drug identified by the United States Drug Enforcement Agency (DEA) as a “Schedule I” drug (see https://www.dea.gov/druginfo/ds.shtml), or any drug identified by the DEA as a Schedule II, III, IV, or V drug unless the individual has a prescription.

7.8.3 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.

7.8.4 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.

7.9 Firearms and Explosives

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

7.9.1 Possession: No persons, without written permission from the CEO or designee, may possess any firearm or explosive within an airport Restricted Area.

7.9.2 All persons, other than those in the excepted classes, to include approved law enforcement officers, 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, 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 a firearm or explosive 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.

7.9.3 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.

7.9.4 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.

7.10 Prohibited Items

7.10.1 With the exception of airport-approved prohibited Items, security badgeholders may not possess or carry items into or within the passenger terminal that are otherwise prohibited by TSA regulation, including the TSA Security Screening Checkpoint. “Prohibited Items” are defined under 49 CFR § 1540.111, and specifically described on TSA’s website at www.tsa.gov/travel/security-screening/whatcanibring/all.

7.10.2 Security badgeholders 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.

7.10.3 Security badgeholders discovering unauthorized or uncontrolled prohibited items must immediately contact OPD Dispatch at (909) 986-6711 to have an officer respond for proper confiscation, disposal, and investigation.

7.10.4 Under no circumstances may hazardous items be disposed of in a trash receptacle.

7.10.5 Airport Approved Prohibited Items: A limited list of items may be considered exceptions if job related. All security badgeholders, 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 and Badging Office for each prohibited item.

7.10.6 Prohibited items must not be left unattended in the passenger terminal unless, as approved by the CEO or designee, the prohibited items are secured and inaccessible to other individuals, to include screened passengers and/or non-security badgeholders. The security badgeholder, 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.

7.10.7 All Sterile Area Concessionaire tenants shall audit Airport-Approved Prohibited Item inventories in conformance with Training of Security Responsibilities (TSR) Sterile Area Concessionaire Requirements.

7.11 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.

7.12 Limitations on Personal Belongings

When entering a restricted area of the airport, all persons are restricted to no more than two (2) personal items (e.g., bag, purse, backpack, tote, messenger bag, computer bag, fanny packs, briefcase, cooler, box, or any other type of container or combination thereof). Additional items, or any one item larger than a standard backpack, must be screened as a delivery by airport officials, or, with prior TSA approval, screened at the TSA Screening Checkpoint. These restrictions do not apply to the transport of medically necessary items.

7.13 Passenger Terminal Deliveries

All deliveries through any airport-controlled door at a passenger terminal (i.e., doors leading from the public area to the sterile area concourse or adjoining secured area ramp) must be inspected by Airport Officials, or, when specifically approved by the TSA, at the TSA Screening Checkpoint.

7.13.1 Deliveries include all merchandise or consumables intended for airport or tenant use within the passenger terminal or secured area ramp, and all merchandise or consumables intended for sale, consumption, and/or use within a passenger terminal, whether to be purchased or obtained from a concession tenant, an airline club or lounge, or at a special event.

7.13.2 Using controlled doors to transport non-inspected deliveries into the sterile area concourse or adjoining secured area ramp is strictly prohibited.

7.13.3 Delivery inspections may include the inspection of delivery personnel and personal belongings.

7.13.4 To schedule a delivery inspection, contact the Airport Security Desk at 909-544-5373.

7.14 Tenant Video Monitoring and Recording Devices

7.14.1 No closed-circuit television (CCTV) system, cameras or other recording devices may be modified, removed, or installed by any tenant or permittee in or around the Airport premises without prior written authorization from the CEO or designee.

7.14.2 Any new CCTV system or camera installation must comply with the OIAA Electronic Security Systems Design & Construction Standards made available from the Security and Badging Office. The CEO or designee must approve the proposed design, features, requirements, and standards. To obtain authorization, tenants and permittees must apply to the Security and Badging Office, specifying the following:

7.14.2.1 Field-of View (FOV) screenshots

7.14.2.2 Video monitoring/recording device model and specifications

7.14.2.3 Recording system and retention time

7.14.2.4 Camera layout drawing

7.14.2.5 Security infrastructure and plan to prevent unauthorized access

7.14.3 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 CEO or designee, is deemed to present a potential risk to Airport security. All subsequent changes or modifications must be submitted to the CEO or designee in writing and approved prior to executing modifications.

7.14.4 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 CEO or designee. No tenant or permittee shall release any video monitoring and/or recording device footage from cameras/devices without prior written authorization from the CEO or designee and, if deemed appropriate, the TSA.

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

7.14.5 Inventory of Video Monitoring and Other Recording Devices: All tenants and permittees shall provide the CEO or designee with an inventory of existing video monitoring and/or recording devices and security plans, including the following:

7.14.5.1 Device manufacturer, model, and specifications

7.14.5.2 Field-of-view

7.14.5.3 Data retention time

7.14.5.4 Placement of video monitoring and/or recording devices

7.14.5.5 Remote access usage

7.14.5.6 Written security plan detailing how unauthorized access will be prevented

7.15 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 strictly prohibited.

7.16 Perimeter Clear Zone

A ten (10) foot clear zone shall be maintained on both sides of the AOA perimeter (fence and walls) to deter and detect unauthorized entry. The clear zone shall remain free of vehicles, stored materials, unattended equipment, or other property. At the owners expense, the CEO or designee may remove, or have removed, such items discovered within posted “no parking” clear zones. As necessary, the ten (10) foot clear zone may be expanded at the sole discretion of the CEO or designee.

7.17 Perimeter Facilities

7.17.1 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.

7.17.2 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.

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

7.17.4 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.

7.18 Unauthorized Individuals, Vehicles and Other Property

7.18.1 At the owners expense, the CEO or designee may remove, or have removed, unauthorized vehicles, stored materials, unattended equipment, or other property discovered within a Restricted Area.

7.18.2 Unauthorized individuals discovered within a Restricted Area shall be removed from the Restricted Area by law enforcement personnel.