Appendix IV – Security Badge Program

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
December 2022	A, B	2-3	Technical Changes
December 2022	F	6-8	Technical Changes
July 2024	All	All	Reformatting & Technical Changes, consolidated Participant & Authorized Signer information from Section 7

Table of Contents

Page is Intentionally Left Blank

Appendix IV- Security Badge Program

IV.1 Security and Badging Office

The Ontario International Airport (ONT) Security and Badging Office (SBO) is responsible for the implementation of Transportation Security Administration (TSA) Rules and Regulations pertaining to the issuance of security badges to persons doing business on Airport property, including persons accessing Airport restricted areas (e.g., Air Operations Area (AOA) and Passenger Terminals), as outlined in Title 49 Code of Federal Regulations (CFR) Part 1542 – Airport Security.

Office Locations

North

Satellite Office
International Arrivals Terminal Lobby
222 International Way, Ontario, CA 91761

South

Main Office
Ontario International Airport Authority
Administrative Building – 1st Floor
1923 E. Avion St., Ontario, CA 91761

Contact Information

Office: (909) 544-5170 – Both Locations
Fax: (909) 937-2513
Email: ontsecuritybadgeoffice@flyontario.com

Hours of Operation

Monday-Friday
8:00 a.m. to 3:30 p.m.
Major holidays observed

Appointments

Schedule your appointments online at
www.flyontario.com/security

IV.2 Participant

IV.2.1 The Ontario International Airport Authority (OIAA) requires all organizations conducting business at ONT, on a permanent or temporary basis, to apply for and maintain the appropriate permit, agreement, or lease with the OIAA.

IV.2.2 Each organization shall become a "Participant" in the Airport Rules and Regulations and the Airport Security Program (ASP) and remain in good standing to retain airport privileges, to include security badges.

IV.2.3 New organizations must be sponsored by an existing Participant, to include the OIAA, to ensure the new organization (e.g., licensee, vendor, or contractor) has a legitimate operational need to conduct business at ONT.

IV.2.4 Sponsoring Participants must immediately notify the SBO when their respective sponsorship is terminated.

IV.2.5 New Company Enrollment Requests may be submitted at www.flyontario.com, at the SBO on a walk-in basis, or by email at ontsecuritybadgeoffice@flyontario.com.

IV.2.6 Whenever a Participant becomes aware of any of the following conditions, the Participant must contact the SBO to verbally request immediate deactivation of the respective security badge. If the SBO is closed, or otherwise unavailable, the Participant must contact the City of Ontario Police Dispatch to verbally request immediate deactivation of the security badge.

IV.2.6.1 A security badge or security key is lost or stolen.

IV.2.6.2 A security badgeholder's employment status changes through employment termination, retirement, or any other form of separation from the company.

IV.2.6.3 An employee is considered a threat for any reason.

IV.2.6.4 A security badgeholder is arrested or convicted of a disqualifying crime pursuant to Airport Rules and Regulations Appendix 4.F Criminal Records Check, or 49 CFR §1542.209.

IV.3 Authorized Signer

IV.3.1 Unless specifically approved by the CEO or designee, each Participant shall designate a minimum of two (2) Authorized Signers, in writing, to include one (1) Primary, and one (1) Alternate. The Primary Authorized Signer shall be the responsive individual for all security badge and/or security key audits performed by the SBO.

IV.3.2 The Authorized Signer 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.

IV.3.3 The Authorized Signer ensures 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 SBO. The Authorized Signer is the primary point of contact between the Participant, the SBO, and other Airport Officials, and shall be directly involved with security violation mitigation and associated corrective action efforts.

IV.3.4 As directed by the CEO or designee, the Authorized Signer shall disseminate and effectively implement applicable security measures for the Participant, as adopted and/or revised by the Airport.

IV.3.5 Authorized Signer Eligibility

IV.3.5.1 Unless specifically approved by the CEO or designee, and, in coordination with the SBO, each Authorized Signer must be a direct employee of the organization; and

IV.3.5.2 Designated on a Letter of Authorization (LOA) from the highest-ranking local official of the organization. If the Authorized Signer changes, a new LOA must be immediately provided to the SBO; and

IV.3.5.3 Pass a Security Threat Assessment (STA) and Criminal History Records Check (CHRC). Participant's designating the Authorized Signer 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

IV.3.5.4 Maintain an active security badge; and

IV.3.5.5 Complete Authorized Signer 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 Signer only sponsoring applicants for a sterile area security badge will only be required to complete sterile area training; and

IV.3.5.6 Submit and maintain an active Authorized Signer Designation Form.

IV.3.6 Authorized Signer Primary Responsibilities

IV.3.6.1 Each Authorized Signer 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 Signer privileges and/or suspension or revocation of the Authorized Signers security badge.

a) Sponsorship Requirements
b) Airport Rules and Regulations
c) Authorized Signer Manual
d) Security Badge and Access Media (Key/Code) Issuance, Accountability, and Audit Procedures
e) CHRC and STA Background Check Procedures
f) Security Badge Training
g) Escort Training
h) Training of Vehicle Search Procedures and Training
i) Security Responsibilities (TSR)
j) Motor Vehicle Operating Permit (MVOP) Procedures
k) Driver's Training and Permit Procedures
l) Security Badge and Key Termination & Recovery Plan
m) Security and Airfield Enforcement Program (SAFE)

n) Stop List Procedures

IV.3.7 Additional Responsibilities

IV.3.7.1 Promptly notify the highest-ranking local official when removed as an Authorized Signer and ensuring an updated LOA is submitted and received by the SBO; and

IV.3.7.2 Maintain required records in accordance with SBO policies and procedures; and

IV.3.7.3 Actively review information and keep abreast of changes in the Security Badging Program; and

IV.3.7.4 Provide the SBO 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

IV.3.7.5 Provide immediate notification to the SBO 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.

IV.4 Security Badges

IV.4.1 The Participant must ensure any person who works or does business on Airport property, on a permanent or temporary basis, has a security badge issued or approved by the Airport, to include Airport public and restricted areas.

IV.4.2 Any person holding an Airport-issued security badge does so as a privilege and not a right. The Airport shall retain ownership of all security badges, and the CEO or designee reserves the right to deny new applicants a security badge, suspend an existing security badge, and, with cause, revoke a security badge and unescorted access privileges.

IV.4.3 Pursuant with this section, each individual is required to pass a Security Threat Assessment and Criminal History Records Check before being issued a security badge.

IV.4.4 Security badges must be used pursuant with this Section, Section 7- Airport Security, Appendix 4 - Security and Airfield Enforcement Program, and the Airport Security Program (ASP). This includes the proper display, access control procedures, and critical requirement to immediately deactivate and return the security badge upon its expiration, a badgeholders' separation of employment, expiration of operational need, or upon demand of Airport Officials.

IV.4.5 The misuse or willful failure to surrender or return a security badge shall be subject to appropriate enforcement under Appendix 4 - Security and Airfield Enforcement Program.

IV.4.6 The SBO will only issue a security badge upon request from the Participants Authorized Signer. On behalf of the Participant, the Authorized Signer is responsible for verifying that each applicant is employed or authorized to perform duties or services on Airport property. The Participant or sponsor of the Authorized Signer and security badgeholder shall remain responsible for the security badgeholder's compliance with these Rules and Regulations.

IV.4.7 Security badge applications must be submitted to the SBO using the Airports identity management system (IDMS) or using the most current fillable forms distributed by the SBO.

IV.4.8 Security badges are issued in varying access levels based upon the Participants 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 by the SBO.

IV.4.9 Customs Seals providing access to a U.S. Customs and Border Protection (CBP) controlled area, to include the Federal Inspection Services Area (FIS), are authorized and issued specifically by the CBP.

IV.5 Initial Security Badge

IV.5.1 The applicant and Authorized Signer must complete, sign, and date the most current application form(s), to include IDMS digital forms; and

IV.5.2 Valid Government-Issued Photo Identification / Employment Eligibility Documents: The applicant must present two (2) valid forms of identification with each application:

IV.5.2.1 Government issued photo identification; and

IV.5.2.2 Employment Eligibility Document pursuant with US Citizenship and Immigration Services (USCIS) Form I-9, List of Acceptable Documents; and

IV.5.3 All applicant biographical information on both forms of identification must be consistent and verifiable. If airfield driving privileges are requested, a valid driver's license must also be presented; and

IV.5.4 As described in this section, the applicant must pass a Criminal History Record Check & Security Threat Assessment. Clearance notifications are provided by the SBO to the respective Authorized Signer. All applicants must complete the badging process, to include applicable training, within thirty (30) calendar days of the clearance notification.

IV.5.5 All applicants must complete required security training and pass the corresponding test(s) to ensure a comprehensive understanding of the Airport Rules and Regulations and the Airport Security Program (ASP).

IV.5.6 As described in Section 9, all applicants requesting to operate a vehicle on the AOA must also successfully pass the ONT AOA Restricted Area Driver Permit Training Program.

IV.6 Security Badge Renewal

Security badges expire on the date printed on the front of the badge and may be renewed up to sixty (60) calendar days prior to the respective expiration date. To renew a security badge, the security badgeholder and Authorized Signer must complete the following:

IV.6.1 Complete, sign, and date the most current application form(s) no more than thirty (30) calendar days prior to the date the form is presented to the SBO.

IV.6.2 The security badgeholder must present two (2) forms of identification. If driving privileges are requested, a valid driver's license must be included.

IV.6.3 As described in this section, the security badgeholder must pass a Criminal History Record Check & Security Threat Assessment. Clearance notifications are provided by the SBO to the respective Authorized Signer. At the discretion of the SBO, the security badgeholder may be required to complete an additional fingerprinting process.

IV.6.4 The security badgeholder must complete required training and pass the corresponding test(s) to ensure a comprehensive understanding of the ONT Rules and Regulations, and the ASP.

IV.6.5 For expired security badges, the employee must be fingerprinted, clear a Criminal History Records Check and have a valid Security Threat Assessment before a security badge can be re-issued.

IV.6.6 If a security badge has expired and was issued with an Aircraft Operator's Criminal History Records Check Certification, the respective air carrier's Authorized Signer must provide a new certification to the SBO and have a valid STA before a security badge can be re-issued.

IV.7 Reasonable Accommodations - Training

Reasonable accommodations may be considered for completing airport security training by submitting a request for accommodations directly to the SBO, at ontsecuritybadgeoffice@flyontario.com, or (909) 544-5170.

IV.8 Security Threat Assessment (STA)

Unless specifically exempted by the TSA, any person requesting a security badge must pass an STA performed by the TSA. Concurrent with the security badge application process, the SBO shall collect and submit the required STA information. Prior to issuance of a security badge, the SBO must receive TSA's confirmation of the applicant's successful completion of an STA.

IV.9 Criminal History Record Check (CHRC)

Unless specifically exempted by the TSA, any person requesting a security badge must be fingerprinted and pass a CHRC. The CEO or designee will conduct a computerized Federal Bureau of Investigations (FBI) CHRC of any individual applying for a security badge, to include renewals. After receiving an applicant's authorization to perform the CHRC, the CEO or designee shall request, receive, and review the criminal history data, if any, to ensure the applicant does not have a conviction for a disqualifying crime, as described in this section, or has been charged with a disqualifying crime and awaiting judicial disposition.

IV.9.1 Aircraft Operator CHRC Certifications:

The CEO or designee may accept a certification from an aircraft operator subject to 49 CFR Part 1544 (Domestic Aircraft Operator) indicating it has complied with the CHRC requirements of 49 CFR §1544.229 for their employees and contractors seeking unescorted access authority. The approved CHRC certification must verify the employee has not been:

IV.9.1.1 convicted,

IV.9.1.2 given a deferred sentence,

IV.9.1.3 found not guilty by reason of insanity,

IV.9.1.4 arrested and awaiting judicial proceedings for any crimes listed in 49 CFR §1542.209; or any felony conviction during the ten (10) years before the date of the individual's application for unescorted access authority, or while the individual has unescorted access authority. If such certifications are authorized and accepted by the CEO or designee, the SBO shall not require the Aircraft Operator to provide a copy of the respective CHRC.

IV.9.2 Disqualifying Criminal Offenses:

As provided by 49 CFR §1542.209(d), any individual has a disqualifying criminal offense if the individual has been convicted, or found not guilty by reason of insanity, of any of the following disqualifying crimes (1-28) in any jurisdiction during the 10 years before the date of the individual's application for unescorted access authority, or while the individual has unescorted access authority.

IV.9.2.1 Forgery of certificates, false marking of aircraft, and other aircraft registration violation; 49 U.S.C. 46306.

IV.9.2.2 Interference with air navigation; 49 U.S.C. 46308.

IV.9.2.3 Improper transportation of a hazardous material; 49 U.S.C. 46312.

IV.9.2.4 Aircraft piracy; 49 U.S.C. 46502.

IV.9.2.5 Interference with flight crew members or flight attendants; 49 U.S.C. 46504.

IV.9.2.6 Commission of certain crimes aboard aircraft in flight; 49 U.S.C. 46506.

IV.9.2.7 Carrying a weapon or explosive aboard aircraft; 49 U.S.C. 46505.

IV.9.2.8 Conveying false information and threats; 49 U.S.C. 46507.

IV.9.2.9 Aircraft piracy outside the special aircraft jurisdiction of the United States; 49 U.S.C. 46502(b).

IV.9.2.10 Lighting violations involving transporting controlled substances; 49 U.S.C. 46315.

IV.9.2.11 Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements; 49 U.S.C. 46314.

IV.9.2.12 Destruction of an aircraft or aircraft facility; 18 U.S.C. 32.

IV.9.2.13 Murder.

IV.9.2.14 Assault with intent to murder.

IV.9.2.15 Espionage.

IV.9.2.16 Sedition.

IV.9.2.17 Kidnapping or hostage taking.

IV.9.2.18 Treason.

IV.9.2.19 Rape or aggravated sexual abuse.

IV.9.2.20 Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon.

IV.9.2.21 Extortion.

IV.9.2.22 Armed or felony unarmed robbery.

IV.9.2.23 Distribution of, or intent to distribute, a controlled substance.

a) Felony arson.
b) Felony involving a threat.
c) Willful destruction of property;
d) Importation or manufacture of a controlled substance;
e) Burglary;
f) Theft;
g) Dishonesty, fraud, or misrepresentation;
h) Possession or distribution of stolen property;
i) Aggravated assault;
j) Bribery; or
k) Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than 1 year.

IV.9.2.24 Violence at international airports; 18 U.S.C. 37.

IV.9.2.25 Conspiracy or attempt to commit any of the criminal acts listed above.

An Authorized Signer receiving an applicant's security badge application and/or CHRC application acknowledging an arrest and conviction for any disqualifying criminal offense described above, shall advise the applicant of their disqualification.

All individuals charged with a disqualifying crime must receive judicial disposition prior to applying for a security badge.

IV.9.3 CHRC Records:

A copy of the criminal record received from the FBI will be provided by the CEO or designee upon written request from an applicant or current security badgeholder. The CEO or designee is the individual's point of contact if he or she has questions about the results of the CHRC.

IV.9.4 CHRC Approval:

A successful CHRC means the employee shall not have been:

IV.9.4.1 convicted,

IV.9.4.2 given a deferred sentence,

IV.9.4.3 found not guilty by reason of insanity,

IV.9.4.4 have been arrested and awaiting judicial proceedings for any crimes listed in 49 CFR §1542.209; or any felony during the ten (10) years before the date of the individual's application for unescorted access authority, or while the individual has unescorted access authority.

IV.9.5 CHRC Denial:

Before making a final decision to deny issuing a security badge, the CEO or designee will provide written notification to the applicant of the following:

IV.9.5.1 The FBI criminal record discloses information that would disqualify him or her from receiving and/or retaining a security badge; or

IV.9.5.2 Based upon the totality of criminal activity disclosed by the FBI criminal record, the CEO or designee has made the determination to deny issuing a security badge.

IV.9.6 Correction of CHRC Records:

Upon receiving the CEO or designee's notification of disqualification, should the applicant believe the FBI criminal record contains inaccurate information, the applicant, within thirty (30) days of receipt, may notify the CEO or designee in writing of his or her intent to correct any FBI criminal record information he or she believes to be inaccurate. The applicant is encouraged to contact the local jurisdiction responsible for the information and the FBI to complete or correct the information contained in his or her record.

IV.9.6.1 If the applicant's written notification of intent to correct FBI records is not received by the CEO or designee within thirty (30) days, the provided written notification of disqualification shall serve as the CEO or designee's final determination to deny issuing a security badge.

IV.9.6.2 If the CEO or designee receives the applicant's notification within thirty (30) days, the applicant, prior to re-consideration of security badge issuance, must provide the CEO or designee with a copy of the revised FBI record and/or certified true copy of the information from the appropriate court. Upon considerations of any revised FBI record and/or certified true copy of the information from the appropriate court, the CEO or designee will either approve the issuance of a security badge or provide written notification to the applicant that a final decision has been made to deny the issuance of a security badge.

IV.9.7 Reporting of Arrests & Disqualifying Criminal Convictions

IV.9.7.1 Security badgeholders must notify the SBO 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 disqualifying crime described in this section.

IV.9.7.2 Upon disclosure by a security badgeholder, or notification from the CHRC program to the airport, of any arrest for a disqualifying criminal offense without indicating a disposition, the CEO or designee shall adjudicate the matter with the security badgeholder, not to exceed forty-five (45) days, to ensure the disposition does not result in a disqualifying offense. After forty-five (45) days, the security badge shall be surrendered to the SBO, which shall be suspended until such time demonstration of judicial disposition is provided by the individual indicating a non-disqualifying criminal offense.

IV.9.8 Surrendering of Security Badge:

Security badgeholders convicted, given a deferred sentence, or found not guilty by reason of insanity for any disqualifying offense, must surrender their security badge to the SBO within twenty-four (24) hours of the disqualifying offense conviction.

IV.10 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 Signer must retrieve the security badge and security key and immediately notify the SBO in person, by phone, or by whatever means possible to ensure that the security badge is immediately deactivated.

IV.10.1 The Authorized Signer must deliver the surrendered security badge and/or security key(s) to the SBO 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.

IV.10.2 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 Participant until the security badge or security key is returned.

IV.11 Lost Security Badge or Security Key

If a security badge and/or a security key is lost, the security badgeholder must immediately notify the SBO 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 Participant responsible for the lost security key.

IV.12 Stolen Security Badge or Security Key

When a security badge or security key is reported stolen, the security badgeholder must immediately notify the SBO by phone to ensure the security badge is immediately deactivated. Replacement badges are issued by the SBO; the security badgeholder 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 SBO 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 Participant responsible for the lost security key.

IV.13 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 CEO or designee to have the fine returned. The CEO or designee 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 CEO or designee may deviate from this policy using evidence of extenuating circumstances or other contributing factors.

IV.14 Security Badgeholders on long term leave

Security badgeholders engaging in a leave of absence for thirty (30) consecutive days or more shall surrender his/her security badge and security keys to their Authorized Signer. Security badgeholders failing to surrender their security badge and keys upon request are subject to the immediate suspension and revocation of their security badge. 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.

IV.14.1 Long Term Leave - Collection and Return of Security Badge: Authorized signatories shall collect and secure all security badges and security keys before badged individuals commence extended leaves of absence. Security badges and security keys shall be provided to the SBO within two (2) calendar days from commencement of leave.

IV.14.2 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 Signer shall notify the SBO by the 30th day that a leave has been extended. The SBO shall immediately suspend security access, and the Authorized Signer shall return Airport property (security badge, keys) to the SBO within two (2) calendar days of such notification.

IV.14.3 Re-entry Following Long Term Leave: When a security badgeholder returns to work from an extended leave, the Authorized Signer shall contact the SBO 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:

IV.14.3.1 CHRC,

IV.14.3.2 STA,

IV.14.3.3 Security training administered by the SBO.