

20 AIRPORT SECURITY RULES AND REGULATIONS

The Rules and Regulations in this Part 20 are adopted by the Manager of Aviation (“the Manager”), pursuant to the Manager’s authority under Article II, Part 11 of the Charter of the City and County of Denver, Chapter 5 of the Denver Revised Municipal Code, and Title 41, Art. 4, Colorado Revised Statutes, in support of the Airport Security Program and to protect the safety of the traveling public consistent with the Federal Transportation Security Administration (TSA) Regulations, including 49 CFR Part 1540, 1542, 1544 et seq., and other applicable federal laws.

20.01 Participant Status

Each Air Carrier, Tenant, Vendor, Ground Transportation (GT) Vendor, Contractor requiring access to the Restricted Area, Sterile Area, and/or Secured Area shall become a “*Participant*” in the Airport Security Program, and remain in good standing in order to retain Airport Security privileges.

20.02 Participant Sponsorship

Any Vendor, GT Vendor or Contractor requiring access to the Restricted Area, Sterile Area, and/or Secured Area must be sponsored by the City & County of Denver (CCD) Department of Aviation, an Air Carrier and/or Tenant. The sponsorship establishes that a Vendor, GT Vendor, or Contractor has legitimate business at the Airport. A company sponsoring a Participant will immediately notify Airport Security when any sponsorship is terminated.

20.03 Authorizing Agent Responsibilities

20.03-1 Each Participant shall designate an Authorizing Agent to ensure the Participant’s compliance with the Airport Security Program and act as the point of contact between the Participant and Airport Security. The Authorizing Agent shall be designated in writing to Airport Security by the Participant.

20.03-2 All Authorizing Agent signatures submitted to Airport Security must match the Authorizing Agent signature on file.

20.03-3 The Authorizing Agent is the primary point of contact for Airport Security, and is responsible for signing all Fingerprinting and Badging Applications, identity verification, Airport ID Badges, Vehicle Permits, Access Changes, Access Control reporting, Driving Privileges, Violation Notice distribution, Quarterly Audits, providing updated current contact information for the company as well as for the Authorizing Agents, and any other business relating to Airport Security.

20.03-4 Each individual designated by a Participant as an Authorizing Agent must successfully complete the following requirements in order to initially qualify, and to maintain qualification, as an Authorizing Agent:

- (a) Attend an initial Authorizing Agent training class and a recurrent Authorizing Agent class annually.
- (b) Maintain an active Airport ID badge at all times.

- (c) Have an Authorizing Agent Designation form signed by a senior company manager and approved by the Director of Security or designee.

20.03-5 Every Authorizing Agent is required to know the policies and procedures outlined in the following sections in the Airport Security Program Participant Manual:

- (a) Airport ID Badges (Colors and types of approved access control media)
- (b) Background Requirements (Criminal History Records Checks and Security Threat Assessments)
- (c) Airport ID Badge Training
- (d) Vehicle Permits (Insurance requirements and types of permits)
- (e) Driver Authorization Training
- (f) Vendor Procedures
- (g) Contractor Procedures
- (h) Badge Audit Procedures
- (i) Violation Notice Procedures and Response required by supervisor personnel
- (j) Access Control Points (Adding access and deleting access from personnel)

20.03-6 Authorizing Agent Signatory Responsibilities for Fingerprinting and Badging Application

- a) The application must be signed by the Authorizing Agent after the employee has completed the employee sections and the backside of the application.
- b) The application must be signed by the Authorizing Agent after the employee has completed the Employee Sections and no more than thirty (30) calendar days before the employee presents the application. All Authorizing Agent signatures must be authentic. Stamped, photocopy, or facsimile signatures will not be accepted on Fingerprinting and Badging Applications.
- b) An Authorizing Agent who signs the Fingerprinting and Badging Application before the Employee Sections have been completed, or if an application is lost and it is not reported to Airport Security, may have his or her Authorizing Agent privileges revoked, and Airport ID Badge may be suspended.

20.04 Entry into Restricted Area

Only individuals who are properly badged or escorted in accordance with the provisions of this Part 20 and applicable federal, state and city laws and regulations shall enter the Restricted Area as necessary in the conduct of flights, inspections or in the course of other official duties.

20.04-1 Approved Identification Media for Access to Restricted Area

Individuals with unescorted access entering the Restricted Area shall display Airport approved identification at all times. The following are Airport approved identification for unescorted entry into the Restricted Area:

- (a) An appropriate Airport ID Badge, as described in this section, issued by Airport Security.
- (b) Federal Aviation Administration (FAA) Flight Standards Inspector Identification (110A). The FAA Form 110A does not provide access; it only affords unescorted movement once access has been achieved by other legitimate means.
- (c) Current and valid Aircraft Operator Media (company-issued picture identification badge), worn by uniformed flight crews.

- (d) A current and valid FAA Airmen Certificate (Pilot's License) along with a picture identification, (e.g., a driver's license), in the possession of a general aviation pilot in the immediate vicinity of his or her aircraft or enroute between aircraft parking and the General Aviation Ramp or Cargo Terminal.
- (e) Official Transportation Security Administration (TSA) credentials. Only TSA Management and Regulatory Inspectors are credentialed.
- (f) Current, valid, and appropriate military identification, carried by military flight crews and military couriers.
- (g) Secret Service credentials. Approved for use during United States Secret Service operations in areas designated by Airport Operations and includes escort privileges.
- (h) Identification meeting the requirements contained in the Airport Emergency Plan, carried by personnel responding to an emergency in the Restricted Area.
- (i) No other forms of identification are approved or authorized.

20.04-2 Approved Identification for Access to the Sterile Area

Individuals with unescorted access entering the Sterile Area shall display Airport approved identification at all times. The following are Airport approved identification for unescorted entry into the Sterile Area:

- (a) An appropriate Airport Identification Badge as described in this Section issued by Airport Security.
- (b) Federal Aviation Administration (FAA) Flight Standards Inspector identification (110A).
- (c) Current and valid Aircraft Operator Media (company-issued picture identification badge), worn by uniformed or non-uniformed flight crews.
- (d) Official Transportation Security Administration (TSA) and Federal Aviation Administration (FAA) credentials. Only TSA Management and Regulatory Inspectors are credentialed.
- (e) No other forms of identification are approved or authorized.

20.04-3 Airport Identification Badges: Classes and Access Areas

All individuals employed at the Airport with Restricted Area access, or working in the Terminal, Concourses, or Parking and Ground Transportation facilities, must obtain an Airport Identification (ID) Badge. Airport ID Badges will be issued by Airport Security. All such identification badges shall be and remain the property of the Airport. The Airport ID Badge must be surrendered on demand to Airport Operations and/or a Contract Security Guard. An individual employed by more than one company, or changing employers, must obtain an Airport ID Badge for each company. Badge color indicates general areas of authorization in relationship with direct support of an individual's job function. Badge color does not determine access. The respective classes of Airport ID Badges, indicated by badge color and associated driving privilege icon, describe driving privileges in direct correlation with their job function.

- (a) Red:
Driving privileges authorized for areas of the airport including the movement area.
- (b) Red Stripe:
Driving privileges authorized for areas of the airport including the movement area with prior approval from Airport Operations and the FAA Control Tower.
- (c) Blue:
Driving privileges authorized for non-movement areas.

(d) Green:

Driving privileges authorized for non-movement areas as assigned by Airport Security.

(e) White:

Driving privileges authorized for service tunnels as assigned by Airport Security.

(f) Yellow:

Driving privileges authorized for non-movement areas as assigned by Airport Security.

(g) Brown:

Driving privileges authorized for driving access to the Ground Transportation (GT) Level (Level 5).

Note: Employees of GT companies working in a tenant leasehold area in the Main Terminal must obtain a White badge.

(h) Pink:

Authorized by Airport Security based on pre-approved “demonstrated need” ONLY.

Restricted Area: Allows “escorted” access (by a current Airport ID Badge holder in accordance with this Part 20) in the Restricted Area for official airport business.

Sterile Area: Allows “Unescorted” access in the Sterile Area for official airport business, once the individual has completed the screening process through a TSA certified screening checkpoint.

Issued by Airport Security personnel or contract security guard personnel in the Airport Office Building reception area. Full Legal Name (First & Last) and Government issued ID (i.e. driver’s license or Passport) is recorded into the Security Visitor badge database.

Requires that the wearer present a valid government-issued picture ID at issue, and carry such an ID while wearing the badge.

Badge expires daily and individuals may be limited to the number of separate issuances. Requests for additional issuances must be approved by the Director/Assistant Director of Security or the Airport Security Coordinator (ASC) on duty or designee.

20.04-4 Application for an Unescorted Access Airport ID Badge

The following must be accomplished in order for an individual to be issued Airport ID Badges granting unescorted access to Restricted and/or Sterile Areas (Red, Red Stripe, Blue, Green, White, and Yellow Badges):

(a) The individual must complete an application, on a form prepared and currently approved by Airport Security. Two valid forms of identification must be presented with the application, one of which must be government issued photo identification. The second form of identification must verify proof of citizenship (i.e., birth certificate or legal residency with work authorization). All information regarding the individual’s name, age, gender, and other vital statistics on both forms of identification must be consistent and verifiable.

(b) An Authorizing Agent of the individual’s employer or the sponsoring tenant must complete a Criminal History Record Check (CHRC) and a Security Threat Assessment (STA) request on each individual who has applied for clearance for unescorted access to the

Restricted Area, and sign the application form indicating that the applicant is not considered a security risk.

(c) If the individual's employer is sponsored by an air carrier under 49 CFR Part 1544, a Fingerprint Certification Form must be signed by the sponsoring air carrier and submitted with the application.

(d) The individual must view a training film on Denver Municipal Airport System Rules and Regulations, as they pertain to overall security, and pass a corresponding test to assure understanding of the Rules and Regulations. If the individual will have Driver Authorization, a valid driver's license must be presented.

(e) The applicant must sign the Fingerprinting and Badge Application indicating:

i) The individual will complete all required Security training programs.

ii) The individual fully understands Denver Municipal Airport System Rules and Regulations, Part 20.

iii) The individual understands, acknowledges, agrees and consents that violations of the security regulations listed in Section 20.04-16, due to the critical nature of these offenses which affect the overall safety and security of Airport employees and the traveling public, are reason for immediate confiscation and suspension (and possible permanent revocation) of the Airport ID Badge and may result in a Denver Police Department (DPD) Municipal Citation.

iv) The individual acknowledges that all Airport ID Badge applicants may be subject to future background investigations by Federal, State or other local judicial or law enforcement agencies.

v) The individual understands that recurrent violations of Denver Municipal Airport System Security Rules and Regulations of a less critical nature will be administered by Part 20.

vi) The individual understands and acknowledges personal responsibility for all violations or fines incurred as a result of his or her own acts or omissions.

vii) An individual, Participant, or Authorizing Agent caught cheating or falsifying any Airport Security document or training may be subject to a Violation Notice and/or a Federal Civil Penalty and/or denial, suspension, or revocation of their Airport ID Badge.

20.04-5 Airport ID Badge Revalidation

(a) Airport ID Badges expire on the date printed on the front of the badge.

(b) The Airport ID Badge may be revalidated up to thirty (30) calendar days prior to the expiration date.

(c) If a 49 C.F.R. Part 1542 Airport ID Badge is suspended because it has expired, the following rules apply.

i) If the employee has cleared a fingerprint-based CHRC and the badge expires a letter, signed by the employee's Authorizing Agent, must be submitted to Airport Security prior to badge reissuance. The letter must be on company letterhead and have the employee's name, badge number, date of hire, and indicate that the employee has been continuously employed since the badge expired. Upon receipt, Airport Security will determine if the employee will be required to undergo a new fingerprint-based CHRC and STA.

- ii) For Airport ID Badges issued under 49 C.F.R. 1542, if the employee has not been continuously employed, the employee must be fingerprinted and clear a CHRC before the badge can be reissued.
- (d) If a 49 C.F.R. Part 1544 Airport ID Badge is suspended because it has expired, the following rules apply.
 - i) If the employee has cleared a fingerprint based CHRC, an STA, and has been continuously employed, an Application signed by the air carrier Authorizing Agent and it must be submitted in advance to the Airport Security office. Upon receipt, Airport Security will determine if the employee will be required to undergo a new STA.
 - ii) For Airport ID Badges issued under 49 C.F.R. 1544, if the employee has not been continuously employed, the employee must be fingerprinted and clear a CHRC before the badge can be reissued.

20.04-6 Criminal History Record Check (CHRC) & Security Threat Assessments (STA)

- (a) 49 CFR Part 1542 Employees (Non-Aircraft Operators)
 - i) Any person requesting or requiring a badge that would permit unescorted access to the Sterile and/or Restricted Areas must be fingerprinted and pass a CHRC and STA. Passing a CHRC means the employee shall not have been convicted, given a deferred sentence, found not guilty by reason of insanity or have been arrested and are awaiting judicial proceedings of any felony crimes listed in 49 C.F.R 1542.209 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.
 - ii) All applicants with criminal records are subject to review and Denver International Airport reserves the right to confiscate and/or revoke an Airport ID Badge and/or deny a Fingerprinting and Badge Application for any criminal activity.
 - iii) All applicants for Airport ID Badges must complete the badging process within thirty (30) calendar days of clearing their CHRC and STA.
 - iv) Any individual possessing an Airport ID Badge must report to his or her supervisor or Authorizing Agent, within twenty-four (24) hours, if she or he has been convicted, given a deferred sentence, found not guilty by reason of insanity or has been arrested and is awaiting judicial proceedings of any felony charge.
 - v) Upon being informed of his or her employee's conviction, deferred sentence, notice of being found not guilty by reason of insanity or the employee has been arrested and is awaiting judicial proceedings of any felony charge, the employee's supervisor or Authorizing Agent must contact Airport Security within twenty-four (24) hours to determine the status of the individual's Airport ID Badge.
- (b) 49 CFR Part 1544 Employees (Aircraft Operators and those sponsored by Air Carriers)
 - i) Any person requesting or requiring a badge that would permit unescorted access to the Sterile and/or Restricted Areas must be fingerprinted and pass a CHRC and STA. Passing a CHRC means the employee shall not have been convicted, or found not guilty by reason of insanity, or arrested for any of the disqualifying crimes and awaiting judicial proceedings of any of the felony crimes listed in 49 C.F.R. 1542.209.
 - ii) All applicants for Airport ID Badges must complete the badging process within thirty (30) calendar days of clearing their CHRC and STA.

- iii) Any individual possessing an Airport ID Badge must report to his or her supervisor or Authorizing Agent, within twenty-four (24) hours, if he or she is convicted, or found not guilty by reason of insanity, or arrested for any of the disqualifying crimes and awaiting judicial proceedings of any felony crimes listed in 49 C.F.R. 1542.209.
 - iv) Upon being informed of his or her employee's conviction, or a finding of not guilty by reason of insanity of any of the felony crimes listed in 49 C.F.R. 1542.209, the employee's supervisor or Authorizing Agent must contact Airport Security within twenty-four (24) hours to suspend the individual's Airport ID Badge.
- (c) 49 CFR Part 1546 Employees (Foreign Air Carrier Operators)
 - i) Any person requesting or requiring a badge that would permit unescorted access to the Sterile and/or Restricted Areas must be fingerprinted and pass a CHRC and STA. Passing a CHRC means the employee shall not have been convicted, or found not guilty by reason of insanity, or arrested for any of the disqualifying crimes and awaiting judicial proceedings of any of the felony crimes listed in 49 C.F.R. 1542.209.
 - ii) All applicants for Airport ID Badges must complete the badging process within thirty (30) calendar days of clearing their CHRC and STA.
 - iii) Any individual possessing an Airport ID Badge must report to his or her supervisor or Authorizing Agent, within twenty-four (24) hours, if he or she is convicted, or found not guilty by reason of insanity, or arrested for any of the disqualifying crimes and awaiting judicial proceedings of any felony crimes listed in 49 C.F.R. 1542.209.
 - iv) Upon being informed of his or her employee's conviction, or a finding of not guilty by reason of insanity of any of the felony crimes listed in 49 C.F.R. 1542.209, the employee's supervisor or Authorizing Agent must contact Airport Security within twenty-four (24) hours to suspend the individual's Airport ID Badge.

20.04-7 Application for a Ground Transportation Airport ID Badge

The following must be accomplished in order for an individual to be issued an Airport ID Badge granting unescorted operation of a motor vehicle on level 5 of the Main Terminal (Brown Badge):

- (a) The individual must complete an application, on a form prepared and currently approved by Airport Security. This form must be signed by the applicant's Authorizing Agent and presented with two valid forms of identification, one of which must be government-issued photo identification. The second form of Identification must prove proof of citizenship or legal residency with work authorization (i.e., birth certificate, passport, etc.).
- (b) Any person requesting or requiring a badge that would permit unescorted access to the GT Level 5 of the Main Terminal must be fingerprinted and pass a five (5) year CHRC and STA. Passing a CHRC means the employee shall not have been convicted, given a deferred sentence, found not guilty by reason of insanity or have been arrested and are awaiting judicial proceedings of any felony crimes listed in 49 C.F.R 1542.209 during the five (5) years before the date of the individual's application for unescorted access authority, or while the individual has unescorted access authority.
- (c) All applicants with criminal records are subject to review and Denver International Airport reserves the right to confiscate and/or revoke an Airport ID Badge and/or deny a Fingerprinting and Badge Application for any criminal activity.

- (d) All applicants must complete the badging process within thirty (30) calendar days of clearing their five (5) year Criminal History Records Check.
- (e) Any individual possessing an Airport ID Badge must report to his or her supervisor or Authorizing Agent, within twenty-four (24) hours, if she or he has been convicted, given a deferred sentence, found not guilty by reason of insanity or has been arrested and is awaiting judicial proceedings of any felony charge.
- (f) Upon being informed of his or her employee's conviction, deferred sentence, notice of being found not guilty by reason of insanity or the employee has been arrested and is awaiting judicial proceedings of any felony charge, the employee's supervisor or Authorizing Agent must contact Airport Security within twenty-four (24) hours to determine the status individual's Airport ID Badge.

20.04-8 Violation Notice Program and Appeals Process

(a) Violations of Security Advisories, Denver Municipal Airport System Rules and Regulations, Manager Directives, and DIA Standard Policies and Procedures regarding Airport Safety, Security, and Operations can be issued by the Manager of Aviation, Deputy Manager of Aviation - Operations, Assistant Deputy Manager of Aviation - Aviation Operations Manager, Assistant Aviation Operations Manager, Director of Security and his or her staff, Airport Operations Representative Supervisors and their staff, Contract Security Guards and Denver Police Department (DPD) officers assigned to Denver International Airport may issue a Violation Notice. Each individual who is issued an Airport ID Badge shall comply with all Security Advisories, Denver Municipal Airport System Rules and Regulations, Manager's Directives, and DIA Standard Policies and Procedures regarding Airport Safety, Security, and Operations. The failure of any individual to comply with such Security Advisories, rules and directives will result in the issuance of a Violation Notice and may result in the assessment of a Federal Civil Penalty and/or the denial, suspension, or revocation of Airport ID Badges.

(b) The Violation Notice is a three part form:

- i) The pink copy is given to the offender who is required to give the Violation to his or her supervisor. The pink copy under certain circumstances may be sent via email and/or U.S. Mail with the white original. The two other copies are sent to the Assistant Director of Security or designee by the issuing agent.
- ii) The Assistant Director of Security or designee sends via email and/or U.S. Mail the white original to the Authorizing Agent or Senior Company Manager of the company for their follow up. A letter will be included informing the Authorizing Agent or Senior Company Manager of the severity of the Violation and the possible consequences of the offender if they receive another Violation Notice in the future.
- iii) The file copy is reviewed by the Assistant Director of Security or designee, and pertinent information is entered into the Violation Notice computer database.
- iv) The Authorizing Agent or Senior Company Manager must ensure that appropriate action is administered against the offender, complete the "Action Taken" section on the white copy and return it via email and/or U.S. Mail to the Assistant Director of Security or designee within ten (10) business days. If the prescribed time frame is not met, the individual who received the Violation may have his or her Airport ID badge suspended until a response is received.

(c) The City and County of Denver reserves the right to deny or to revoke an Airport ID Badge based upon reasonable grounds after giving due consideration to the sensitivity of the level of access and the areas to which the individual has actual access and the nature of the offense which forms the basis of the denial or revocation. Violations severe enough to require revocation under this section include, but are not limited to, those described in 20.04-16.

(d) When the holder of an Airport ID Badge is issued a Violation Notice of a less than critical nature, he or she may, within ten (10) business days thereafter, request a meeting with the Assistant Director of Security or designee in writing, to review the facts giving rise to the Violation Notice. If such meeting is not requested, the Violation Notice will become final, and the badge holder will have waived all rights to review or appeal thereof. If such a meeting is timely requested, the Assistant Director of Security or designee shall conduct an informal meeting with the person who was issued the Violation Notice. At such meeting, the Assistant Director of Security or designee shall give such person the opportunity to present facts and arguments, if any, as to why the Violation Notice was not properly issued, and shall consider the facts in support of the Violation Notice. The Assistant Director of Security or designee shall then decide whether the Violation Notice should be withdrawn. If the Violation Notice is withdrawn, such fact may be communicated orally to the person to whom it was issued. If the Violation Notice is not withdrawn and/or not appealed in a timely fashion, the violation will be considered valid and entered into the Violation Notice data base.

(e) When the holder of an Airport ID Badge is issued a second Violation Notice which is substantively the same as another Violation issued to the same individual within a two (2) year period, a Violation Notice Hearing will be conducted by the Assistant Director of Security or designee. A pre-Hearing letter will be sent via email and/or U.S. Mail informing the Authorizing Agent or Senior Company Manager that a Hearing needs to be scheduled with Airport Security within ten (10) business days and that a management representative or Authorizing Agent of the company/department must attend along with the employee. If the prescribed time frame is not met, the individual who received the Violation may have his or her Airport ID badge suspended until a Hearing takes place. If following this Hearing, the Assistant Director of Security or designee determines that the violation is valid, the Assistant Director of Security or designee shall communicate his or her decision in writing to the individual who was issued the Violation Notice, stating any violations which the Assistant Director of Security or designee reasonably believes were committed by such individual and the consequences for such violations. Such decision (except a decision to withdraw a Violation Notice) may be appealed as detailed in 20.04-8 (g).

(f) A third Violation in the same category by a company may result in the suspension of badging privileges until the manager of the violating company provides proof to the Director or Assistant Director of Security that the Violation will not occur again.

(g) If an application for an Airport ID Badge is denied or an Airport ID Badge is suspended or revoked, the individual who has been denied a badge or who has had his or her badge suspended or revoked during a Violation Notice Hearing may request an administrative hearing by contacting the Director of Security in writing who will serve as the Appeals Officer within thirty (30) calendar days after the date of such denial or revocation. The hearing shall be conducted as expeditiously as possible, and in accordance with any rules adopted by the Appeals Officer for such proceedings. Evidence shall be submitted under oath or affirmation. The petitioner shall bear the risk of non-persuasion, and the standard of proof

shall conform to that in civil non-jury cases in Colorado State District Courts. The Appeals Officer shall thereafter make a final determination as to the action being appealed. Such final determination may be reviewed under Rule 106(a)(4) of the Colorado Rules of Civil Procedure. A request for reconsideration of the determination may be made if filed in writing with the Deputy Manager of Aviation/Operations within fifteen (15) calendar days of the date of determination, in which case the Deputy Manager of Aviation/Operations shall review the record, and the determination shall be considered a final order of the Deputy Manager of Aviation/Operations on behalf of the Manager of Aviation upon the date when the Manager rules on the request for reconsideration.

(h) An employee requesting an Airport ID Badge must resolve all pending or valid violations before being allowed to proceed in the badging process. If the employee no longer works for the company and is attempting to be employed by a different company, a management representative from the “new” company must attend the Violation Notice Hearing along with the employee.

20.04-9 Airport Security Program Participant

(a) No participant of the Airport Security Program shall divulge the Airport Security Program Participant Manual or any other security source documents to any individual, unless the individual has a specific and valid need to know such information, as identified and defined in the federal government’s Transportation Security Regulations and (TSA) 49 C.F.R. Parts 15 and 1520.

20.04-10 Termination of Employees; Return of Badges and Security Keys Issued by Airport Security

(a) It is the responsibility of the employer of any person to whom an Airport ID Badge or Security keys has been issued to immediately notify Airport Security when an employee is separated from the company for any reason, or loses his or her Airport ID Badge or Security Keys.

(b) All Airport ID Badges and Security Keys shall be surrendered to Airport Security within ten (10) business days when any employee or other individual required to have such identification badge: terminates employment; is transferred to another location; or when the project or contract under which that individual is working is completed or terminated.

(c) A fee for costs shall be assessed against the employer who fails to return the Airport ID Badge or Security Keys within thirty (30) calendar days upon the termination of the individual’s employment, transfer, or completion of the project or contract.

(d) If a badge is terminated and not surrendered to Airport Security under 20.04-10(b), all other badges and Security Key(s) issued to that individual may be suspended and no additional badges or Security Key(s) may be issued to that individual until the terminated badge or Security Key(s) are returned to Airport Security.

20.04-11 Fees for Airport ID Badges & Security Keys

There shall be a fee to cover the administrative cost of producing the Airport ID Badge. An additional fee may be requested to cover the administrative cost of processing a lost badge or Security Key(s).

20.04-12 Display and Care of Airport ID Badge, Security Key(s) and Access Pin & Cipher Code Numbers

- (a) All individuals in the Restricted Area and any other area where an Airport ID Badge is required must display on their person at all times their Airport ID Badge or other approved identification as defined in these rules. The Airport ID Badge or other approved identification shall be worn on the front upper half of the body so that the picture is visible and not covered with other identification.
- (b) With the intent of preventing unauthorized use of Airport ID Badges and Security Key(s), all individuals to whom such a badge and/or Security Key(s) have been issued shall store their badge and/or Security Key(s) in a secure place in their possession and under their control at all times.
- (c) Badge holders will not subject their Airport ID Badge to extreme environmental elements.
- (d) Any individual who is issued Access Pin and/or cipher code number(s) will ensure that it is kept in his or her immediate control to prevent unauthorized use of the Access Pin number and will ensure his or her Access Pin and/or cipher code number(s) is never stored in close proximity to his or her Airport ID Badge.
- (e) Each individual will be allowed up to three (3) replacement Airport ID badges and/or Security Key(s) if the badge and/or Security Key(s) have been lost or stolen with an increasing replacement cost for each. A subsequent request for a replacement badge and/or Security Key beyond three (3) will require the individual and a management representative of the company to have a Hearing with the Assistant Director of Security or designee. At this Hearing, a determination will be made whether Airport Security will issue another Airport ID badge and/or Security Key(s) to the individual.

20.04-13 Escorting in the Restricted Area or other Secure Areas

- (a) Escorting in the Restricted Area is permitted by Red, Red Stripe, Blue, Yellow or White Airport ID Badge holders only.
- (b) An escorting badge holder must keep individuals under his or her escort, in view and under his or her control at all times.
- (c) For every six (6) unbadged individuals under escort, there must be at least one (1) escorting Airport ID Badge holder (6:1 ratio). Airport Security managers and certain Airport Operations Division managers (Assistant Aviation Operations Managers and above) may approve different escort ratios for special events.
- (d) Escorting is not allowed at turnstile locations.
- (e) Non-badged individuals will be allowed to be escorted up to three (3) days into the Restricted Area and/or Sterile Area for official business only. Individuals who require more than three (3) daily escorts must be badged or have approval from the Director of Security or designee.
- (f) Employees who are awaiting CHRC and STA clearances are not allowed to be escorted into the Restricted Area and/or Sterile Area.

20.04-14 Challenging and Reporting Unauthorized Persons

- (a) Each individual who has been issued an Airport ID Badge is responsible for challenging any individual who is in the Restricted Area or any area where an Airport ID Badge is required and is not wearing an approved Airport ID Badge required for access to the area. An individual who does not challenge an apparently unauthorized person and is observed by

Airport Security and/or TSA Transportation Security Inspectors will be cited for noncompliance.

(b) Any individual challenged who cannot produce proper identification as defined in Rule 20.04-1 must be identified and reported to Airport Operations immediately.

20.04-15 Right to Revoke an Airport Id Badge

All Airport ID badge holders and applicants are subject to review by local and Federal Law Enforcement, Department of Homeland Security (DHS) agencies, Airport Legal Services and Airport Security. Denver International Airport has the right to confiscate and/or revoke an Airport Id Badge (or deny an application) for criminal activity (e.g. certain misdemeanors and/or felony convictions) or perceived threats against the airport, passengers or employees.

20.04-16 Critical Violations “Big 6”

No individual to whom an Airport ID Badge or Security Key(s) (including Intellikey(s)) has been issued shall intentionally perform any of the following acts. The intentional commission of any such acts, due to their critical negative effect on the safety and security of Airport employees and the traveling public, is reason for immediate confiscation and suspension (and possible permanent revocation) of the Airport ID Badge, issuance of a Violation Notice, and a Violation Notice Hearing in accordance with Section 20.04-8:

- (a) Loaning (or borrowing) the Airport ID Badge or Intellikey to anyone under any circumstances;
- (b) Allowing unauthorized individuals or vehicles into the Restricted Area;
- (c) Blocking and/or damaging doors, gates, or card readers, and/or leaving doors or gates open that could be a Restricted Area access route for unauthorized individuals;
- (d) Bypassing the security system, passing back an Airport ID Badge or Intellikey, or providing access to unauthorized individuals;
- (e) Altering the Airport ID Badge; or
- (f) Interfering with security screening, security procedures, and personnel.

20.04-17 Other Violations

Violations other than those listed in Section 20.04-16 shall also be administered in accordance with the provisions of Section 20.04-8. These Denver Municipal Airport System Rules and Regulations will be published at <http://www.flydenver.com> for review by all Airport tenants and companies whose employees have been issued Airport ID Badges, and each such company and its employees are responsible for knowledge of the contents of these Rules and Regulations.

20.04-18 Civil Penalties Imposed by Transportation Security Administration (TSA)

Any employer not regulated under 49 C.F.R. Part 1544, Aircraft Operator, will be responsible for payment or reimbursement to the City & County of Denver of any Civil Penalties imposed by the Transportation Security Administration (TSA) for individual security violations by their employees for violations under 49 C.F.R. Part 1542.

An employee may be personally subject to Civil Penalties imposed by the Transportation Security Administration (TSA) for individual security violations they commit under 49 C.F.R Part 1542.

20.05 Submission to Screening and Use of Screening Services, and the Use of Advanced Systems

20.05-1 No individual, except law enforcement or TSA officers, may enter a Sterile Area without submitting to the screening of his or her person and property in accordance with the procedures being applied to control access to that area under applicable Federal Regulations.

20.05-2 Pre-screened charter and scheduled operations are permitted direct access to a concourse in the Sterile Area if the following criteria are met.

(a) Screening of individuals permitted such access by the TSA must have been performed in a commercial passenger airport terminal, and

(b) Limited Essential Air Service (EAS) route substitute mode of transportation and all restrictions thereupon, as approved by the TSA, is utilized.

20.05-3 Companies will ensure employees submit to screening and the use of biometrics and other advanced technologies as required. Employees refusing to submit to advanced systems and procedures are subject to a Violation Notice and/or confiscation and suspension (and possible permanent revocation) of their Airport ID Badge in accordance with Section 20.04-8.

20.06 Three-Foot Clear Zone

A clear zone of three (3) feet is established for both sides of all security fences around the Restricted Area. The clear zone must not contain any object which could be of assistance to an individual trying to scale a fence. Tenants of the Airport who control security fences by way of a Security Agreement with the Airport are responsible for keeping the clear zones in their area free of obstacles. Failure to comply with the Three-Foot Clear Zone is subject to the Violation Notice Program and/or monetary penalties for failure to comply (Section 1.13.8).

20.07 Use of Airport Entrances, Gates, and Doors

20.07-1 All badged employees shall enter the Airport by authorized entrances.

20.07-2 Emergency exit fire doors in the terminal and concourses will be used only in the event of an emergency requiring use of these doors. The only exception is when operational requirements demand use of an emergency door and an Airport ID Badge is used for access. Requests for authorized access will be considered by the Director of Security or designee for approval.

20.07-3 It shall be the responsibility and duty of air carriers and tenants, and their personnel, to close and secure gates and doors in the terminal and concourse areas when not in use.

20.07-4 No badged employee issued a Personal Identification Number (PIN) and/or cipher code shall write or verbally announce in a public manner the number/code since it may lead to unauthorized access.

20.07-5 When an authorized badged employee accesses a door, gate, or elevator leading to or from the Restricted Area, it is the individual's responsibility to ensure that unauthorized individuals do not gain access to the Restricted Area.

20.07-6 When any contract security guard is in control of a door, gate, or elevator leading to or from the Restricted Area, it is the contract security guard's responsibility to ensure that unauthorized individuals or vehicles do not gain access to the Restricted Area. This applies to contract security guards physically located at the access point as well as any contract security guard who controls a gate from remote locations.

20.07-7 No pedestrian traffic is allowed in the service tunnels.

20.07-8 When driving through a gate leading to or from the Restricted Area, the driver must remain at the gate until the gate is fully closed in order to prevent unauthorized individuals or vehicles from

going through the gate to the Restricted Area. If, while the gate is open, another individual, unauthorized or authorized but not using their Airport ID Badge, attempts to pass through that gate (“tailgating”), the individual who opened the gate by card access must identify, prevent (to the extent possible without physical contact), and report the individual(s) who attempted to tailgate them through the gate.

20.07-9 When accessing or controlling a non-access control door, gate, or elevator leading to the Restricted Area, the individual accessing or controlling the access point must challenge and request Airport-approved identification from all persons who attempt to gain access in order to assure that they are authorized. When accessing or controlling an access control door, gate or elevator leading to the Restricted Area, the individual accessing or controlling the access point must not permit an individual to gain access unless that individual successfully uses their Airport ID Badge in the access control reader. If any badge holder determines that an access control reader or door is inoperative, that individual must immediately notify the Airport Communications Center and stand by until Airport Operations and/or contract security personnel arrives on scene and allows the badge holder to leave. If an unauthorized individual attempts to gain access, or actually gains access, the individual controlling access must identify, prevent (to the extent possible without physical contact), and report the unauthorized individual to Airport Operations immediately.

20.07-10 When an authorized individual accesses an access control door, only that individual may pass through the door. The individual must assure that only they pass through the photo cell on the door during the timed opening of the door (approximately thirty seconds). Group escorting is not authorized unless the group remains under continuous escort of the individual who cards the access control door. If, while the door is open, another individual, unauthorized or authorized but not using their Airport ID Badge, attempts to pass through that door (“tailgating”), the individual who opened the door by card access must identify, prevent (to the extent possible without physical contact), and report the individual(s) who attempted to tailgate them through the door. The last individual to use the door by access control through which illegal entry occurred will be cited for a violation of this rule if he or she does not identify, prevent (to the extent possible without physical contact), and report the individual(s) attempting to tailgate to Airport Operations immediately.

20.07-11 No pedestrian traffic is allowed through any vehicle Guard Gate (i.e. Gate 1, 5, etc.) or vehicle perimeter gate (i.e. P10, P42, etc.) accessing the Restricted Area.

20.07-12 Escorting in the Restricted Area is permitted by Red, Red Stripe, Blue, Yellow or White Airport ID Badged individuals only. Individuals not having access control door disable authorization will be required to press the Help button at the entry access control location and obtain permission and assistance from the Airport Communications Center. To return to the interior of a building from a Restricted Area with individuals under escort, the authorized Airport ID Badge holder must open the door by the outside access control reader, pass through the photo cell and press the Help Button on the inside access control reader to obtain permission from the Airport Communications Center to bring escorted individual(s) back through the photo cell and out of the Restricted Area.

20.07-13 All Airport ID Badged employees in a vehicle entering a guarded security access gate which has an access control reader shall show their Airport ID Badge to the guard on duty. Passengers of the vehicle without an Airport ID Badge must show a government-issued picture ID and be entered into the escort program database (See 20.04-13e for number of times allowed). All Airport ID Badges will be carded on the access control reader or compared to the Stop List. The guard will also conduct a comparison of the badge picture to the person and verify the expiration date of the badge.

20.07-14 Any badged employee guarding a Restricted Area access point must be in uniform, display an Airport ID Badge, have a radio or telephone for emergency communications, have a current Stop List issued by Airport Security, and written Post Orders.

20.07-15 Any badged employee operating or using a bag belt who fails to secure it after use will be issued a Violation Notice.

20.07-16 Any badged employee controlling or operating a jetway boarding door must access using the access control reader before boarding passengers. If a passenger opens the door from the Restricted Area and the door time open expires, the badged employee controlling the boarding will be issued a Violation Notice.

20.08 Use of Airport Federal Inspection Services (FIS) Facilities

20.08-1 All badged personnel in the FIS facilities during International Flight processing must have an FIS seal displayed on their Airport ID Badge, or be a City & County of Denver badged employee with a working demonstrated need to be in the FIS Facility. The FIS seal does not have escort privileges. Employees with access privileges or an approved Customs and Border Protection (CBP) FIS seal may not bypass FIS screening while arriving or departing Denver International airport via an international flight.

20.08-2 No individual shall open a non-international access point door during an International Flight, providing access out of the FIS sterile area.

20.08-3 No individual shall bypass the security screening checkpoints via the FIS facility.

20.08-4 No FIS doors may be propped open at any time, except for the emergency exit doors entering into the International nodes.

20.08-5 All personnel displaying an approved FIS seal are authorized to be in the FIS facilities ONLY during those times which their job requires them to be in the FIS facility.

20.08-6 Contractor must be escorted at ALL time in the FIS facility by CBP or Airport Operations personnel.

20.08-7 Bag belts may not be used as a means of entering the FIS facility.

20.08-8 It is the employer's responsibility to ensure all employees with job titles that have AIJ and/or TFF access groups have an FIS seal.

20.08-9 All individuals who require an FIS seal must complete the application process conducted by the Customs and Border Protection (CBP) Office.

20.09 Conduct on Airport Property

Any individual on Airport Property who's actions and/or behavior is not compliant with any of Denver Municipal Airport System Rules and Regulations may have their Airport ID Badge and/or Security Key(s) confiscated and suspended pending a hearing in accordance with Section 20.04-8.

20.10 Weapons in the Restricted Area and/or Sterile Area

20.10-1 ONLY active, on-duty Denver Police (DPD) officers or federal law enforcement officers will be allowed access via the Access Control System to the Restricted Area and/or the Sterile Area with a weapon in lieu of Security Checkpoint screening. Retired law enforcement officers, licensed guards, and persons possessing a concealed carry permit issued by any entity are expressly not allowed into the Restricted Area and/or the Sterile Area with a weapon.

20.10-2 All off-duty law enforcement officers and Federal Flight Deck Officers (FFDO) accessing the Sterile Area must enter through an approved TSA security check point and follow TSA established credential verification and sign-in procedures.

20.10-3 On-duty Law Enforcement Officers on official business and under escort by Denver Police (DPD) may enter the Restricted Area. This escort must be approved by either the Director of Security or the Denver Police Department Airport Commander.

20.11 Contraband in the Restricted Area and/or the Sterile Area

Items listed on the Prohibited Items page of the TSA web site (www.tsa.gov) and items listed as hazardous materials regulated by the FAA located on the FAA web site (www.faa.gov) are forbidden to be in the Restricted Area and/or Sterile Area. As well as, any other item deemed as contraband by local law enforcement authorities. Flammable liquids must be transported in a proper container and in an authorized vehicle. Contraband may not be transported into the Restricted Area and/or Sterile Area on employee busses, or stored in employee lockers.

20.12 Photography in the Sterile and Restricted Areas

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 the sterile and/or restricted area is prohibited.

20.13 Unattended Baggage or Articles

Unattended baggage and/or articles are prohibited in all areas of Denver International Airport. If unattended baggage or articles are found, they are subject to search and may be confiscated by Denver Police Department (DPD) or TSA personnel and may be destroyed.

NOTICE

The Rules and Regulations of the Denver Municipal Airport System are provided on the website of Denver International Airport, www.flydenver.com, as a convenience to the public. Copies may also be obtained from the Department of Aviation's Technical Services Office. The City Clerk is the official custodian of all City rules and regulations under the Revised Municipal Code of the City and County of Denver, sections 2-91 to 2-100. Official, current versions of these rules and regulations may be obtained at the City Clerk's office. For the Clerk's office location and hours, visit the City's website, www.denvergov.org.

Revised Effective June 1, 2011