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 (ASP) and to protect the safety of the traveling public consistent with the Federal Transportation Security Administration (TSA) Regulations, including Title 49 Code of Federal Regulations (CFR) Part 1540, 1542, 1544 et seq., and other applicable federal laws.

20.00 Key Definitions and Acronyms

**Airport Security Coordinator:** (ASC) As detailed in Title 49 CFR § 1542.3, “Each airport operator must designate one or more Airport Security Coordinators (ASC) in its security program...that serve as the airport operator’s primary and immediate contact for security-related activities and communicates with TSA...is available to TSA on a 24-hour basis...review(s) with sufficient frequency all security-related functions to ensure...compliance...and immediately initiate(s) corrective action for any instance of non-compliance...review(s) and controls the results of employment history, verification, and criminal history records checks”.

**Airport Security Program:** (ASP) As defined in Title 49 CFR § 1540.5, “A security program approved by TSA under Title 49 CFR § 1542.101.

**Authorized Signatory:** The individual(s) or designated representative of a company/department authorized to sponsor individuals and request airport personal identification media (i.e. Airport ID badges), who are the primary point of contact for Airport Security. At DEN, these designated company representatives were also referred to as “Authorizing Agents”.

**City and County of Denver:** (CCD) The Airport Operator for Denver International Airport (DEN).

**Controlled Area:** Any area on airport property not designated as a Secured or Sterile Area, where access has been or can be limited or restricted as determined by the Director of Security or designee. Demarcation of controlled areas may include but is not limited to: signage, the access control system, security keys, or the presence of security personnel.

**DEN:** The official acronym for Denver International Airport that is recognized by the Transportation Security Administration and Federal Aviation Administration.

**Escort:** As defined in Title 49 CFR §1540.5, “To accompany or maintain constant visual contact with an individual who does not have unescorted access authority into or within a secured area”. At DEN, the individual must also be kept under control at all times.

**Federal Aviation Administration:** (FAA) A federal entity that is under the umbrella of the United States Department of Transportation which, among other responsibilities, has regulatory oversight over US airports.

**Participant:** An aircraft operator, foreign air carrier, tenant, contractor, vendor, Ground Transportation (GT) vendor or CCD section that has security obligations at DEN.

Denver Municipal Airport System Rules and Regulations
Source: Official Web site of Denver International Airport (business.flydenver.com)
**Personnel Identification Media or Identification Media:** Any credential, card, badge or other media issued for identification purposes and use at an airport. At DEN, this is commonly referred to as the “Airport ID badge.”

**Sterile Area:** As defined in Title 49 CFR §1540.5, “...a portion of an airport defined in the airport security program that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA.”

**Secured Area:** As defined in Title 49 CFR §1540.5, “...a portion of an airport specified in the airport security program in which certain security measures....are carried out.” At DEN, this area is also referred to as the “Restrictied Area” and is where aircraft operators and foreign air carriers enplane sort and load baggage and any adjacent areas that are not separated by adequate security measures.

**Stop List:** A current list which identifies individuals who have had their Airport ID badges invalidated, suspended or de-authorized and have not returned their Airport ID badges to DEN.

**Title 49 CFR Part 1520:** Federal regulations regarding the protection of Sensitive Security Information (SSI)

**Title 49 CFR Part 1542:** Federal regulations regarding the aviation security rules governing “airport operators.” The City and County of Denver (CCD) is the “airport operator” for Denver International Airport (DEN).

**Title 49 CFR Part 1544:** Federal regulations regarding the aviation security rules governing “aircraft operators.”

**Title 49 CFR Part 1546:** Federal regulations regarding the aviation security rules governing “foreign air carriers.”

20.01 Participant Status
Each Air Carrier, Tenant, Vendor, Ground Transportation GT Vendor, or Contractor requiring access to the Secured Area, Sterile Area, and/or any other Controlled Areas shall become a “Participant” in the ASP, 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 Secured Area, Sterile Area, and/or any other Controlled Areas must be sponsored by CCD Department of Aviation, an Air Carrier, Tenant, and/or Contractor. 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 that sponsorship is terminated.

20.03 Authorized Signatory Responsibilities

20.03-1 Each Participant shall designate an Authorized Signatory to ensure the Participant’s compliance with the ASP and act as the point of contact between the Participant and Airport

Source: Official Web site of Denver International Airport (business.flydenver.com)
Security. The Authorized Signatory shall be designated in writing to Airport Security by the Participant.

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

20.03-3 The Authorized Signatory is the primary point of contact for Airport Security, and is responsible for the authorization of: all Fingerprinting and Badging Applications, applicant identity verification, active and inactive Airport ID badges, vehicle permits, access changes, access control reporting, driving privileges, violation notices, active badge certification reports, and security key user agreements. The Authorized Signatory is also responsible for maintaining current contact information for the company as well as any other business relating to Airport Security.

20.03-4 Each individual designated by a Participant as an Authorized Signatory must successfully complete the following requirements in order to initially qualify, and to maintain qualification, as an Authorized Signatory:
   (a) Attend an initial Authorized Signatory training class and annual recurrent Authorized Signatory training.
   (b) Maintain an active Airport ID badge.
   (c) Submit and maintain an active Authorized Signatory Designation form.

20.03-5 Every Authorized Signatory is required to know the policies and procedures as they apply to their company:
   (a) Personnel Identification Systems
   (b) Background Check Procedures
   (c) Airport ID badge Training
   (d) Vehicle Permit Procedures
   (e) Driver Authorization Training
   (f) Security Key Procedures
   (g) Audit Procedures
   (h) Violation Notice Response
   (i) Cipher Code Procedures

An Authorized Signatory who fails to follow these procedures may have his or her Authorized Signatory privileges and/or Airport ID badge revoked or suspended.

20.03-6 Authorized Signatory Responsibilities for Fingerprinting and Badging Applications
The application must be signed by the Authorized Signatory after the employee has completed the employee sections and signed the application. The Authorized Signatory’s signature must be dated no more than thirty (30) calendar days prior to the date that the application is presented to Airport Security. All Authorized Signatory signatures must be authentic. Stamped or photocopied signatures will not be accepted. If a Fingerprinting and Badging Application is signed by an Authorized Signatory before the employee sections have been completed, or if an application is lost and is not reported to Airport Security, the Authorized Signatory may have his or her Authorized Signatory privileges and/or Airport ID badge revoked or suspended.
20.04 Entry into Secured Area and Sterile 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 Secured Area or Sterile Area as necessary in the conduct of flights, inspections or in the course of other official duties.

20.04-1 Approved Identification Media for the Secured Area
Individuals with unescorted access authority entering the Secured Area shall display Airport approved identification at all times. In addition to an appropriate Airport ID badge issued by Airport Security and described in this Part, the following are approved identification for unescorted access authority while in the Secured Area:
(a) FAA Flight Standards Inspector Identification (110A).
(b) Aircraft Operator and Foreign Air Carrier personnel identification media (company-issued picture identification badge), worn by uniformed flight crews.
(c) 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.
(d) Official TSA credentials.
(e) Federal Law Enforcement Officer (LEO) credentials.
(f) Identification meeting the requirements contained in the Airport Emergency Plan, for Emergency Response Personnel who are responding to an emergency.

20.04-2 Approved Identification for the Sterile Area
Individuals with unescorted access authority entering the Sterile Area shall display Airport approved identification at all times. In addition to an appropriate Airport ID badge issued by Airport Security and described in this Part, the following are Airport approved identification for unescorted access authority while in the Sterile Area:
(a) FAA Flight Standards Inspector identification (110A).
(b) Aircraft Operator and Foreign Air Carrier personnel identification media (company-issued picture identification badge), as approved by the TSA.
(c) Official TSA and FAA credentials.
(d) Federal Law Enforcement Officer (LEO) credentials.
(e) State and Local Law Enforcement Officer (LEO) credentials.

20.04-3 Approved Identification for Controlled Areas
Individuals who have no Airport ID badge must be accompanied by an Airport ID badge holder while in any Controlled Area.

20.04-4 Airport Identification Badges and Access Areas
All individuals employed at the Airport with Secured Area and/or Sterile access, or working in the Jeppesen Terminal, parking facilities, Ground Transportation facilities, or anywhere else on airport property as determined by the Director of Security or designee, must obtain a DEN Airport ID badge. Airport ID badges will be issued by Airport Security, and shall be and remain the property of DEN. The Airport ID badge must be surrendered on demand to Airport Operations personnel, Denver Police Department (DPD) officers, and/or Contract Security Guards. An individual employed by more than one company, or changing employers, must obtain an Airport ID badge for each
Badge color indicates general areas of authorization and the ability to escort, based on an individual’s job function. Badge color does not determine access control privileges; rather, company and job title will determine what access control profile is created for individual employees. Certain icons may be affixed to Airport ID badges indicating additional authorization (e.g., airfield driving privileges, Federal Inspection Services access), in direct correlation with the employee’s job function. Classes of Airport ID badges issued by Airport Security include:

(a) Secured and Sterile Area Airport ID badges:
   Authorized for unescorted access authority in both the Secured and Sterile Areas. Badge color indicates whether or not the badge holder has escort privileges.

(b) Sterile Area Airport ID badge:
   Authorized for unescorted access authority in the Sterile Area.

(c) Public Area Airport ID badge:
   Authorized for working in the Jeppesen Terminal and other public areas as well as driving access to GT Level 5 of the Jeppesen Terminal.

(d) Sterile Area Visitor ID badge:
   Authorized based on pre-approved “demonstrated need” ONLY, and issued by Airport Security personnel or contract security guard personnel in the Airport Office Building reception area. Requires the presentation of a valid, government-issued photo ID at issue, and that such ID be carried by the badge holder at all times while wearing the badge. The badge must be worn at all times while in the Sterile Area. Requires that the badge holder enter the Sterile Area through a TSA certified screening checkpoint. Expires daily, and the number of separate issuances is limited.

20.04 Application for an Airport ID Badge
The following is required for the issuance of an Airport ID badge.

(a) The individual must complete and sign an application form 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., state-issued 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. If the individual will have airfield or tunnel driving privileges, a valid driver license must be presented.

(b) An Authorized Signatory of the individual’s employer must sign the application.

(c) If the individual’s employer is an air carrier, certification of fingerprinting must also be provided by the employer.

(d) The individual must view a security training film, and, if airfield or tunnel driving privileges is being requested, a driver training film, and pass the corresponding test(s) to assure understanding of the applicable Denver Municipal Airport System Rules and Regulations.

20.04-6 Criminal History Record Check (CHRC) & Security Threat Assessments (STA)
Any person requesting an Airport ID badge must be fingerprinted and pass a CHRC and STA.

(a) For Title 49 CFR Part 1542 (Airport Operator or Airport Operator sponsored) employees requesting unescorted access authority to the Secure and /or Sterile areas, passing a CHRC means the employee shall not have been convicted of, given a deferred sentence, found not
guilty by reason of insanity or have been arrested and be awaiting judicial proceedings for any crimes listed in Title 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.

(b) For Title 49 CFR Part 1544 or Part 1546 (Aircraft Operators) employees, passing a CHRC means the employee shall not have been convicted of, given a deferred sentence, found not guilty by reason of insanity or have been arrested and be awaiting judicial proceedings for any crimes listed in Title 49 CFR 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.

(c) For employees requesting unescorted access authority to operate a commercial motor vehicle on Level 5 of the Jeppesen Terminal, passing a CHRC means the employee shall not have been convicted of, given a deferred sentence, found not guilty by reason of insanity or have been arrested and be awaiting judicial proceedings for any crimes listed in Title 49 CFR 1542.209, or any felony, 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.

(d) All applicants with criminal records are subject to review and DEN reserves the right to confiscate and/or revoke an Airport ID badge and/or deny a Fingerprinting and Badging Application for any criminal activity.

(e) All applicants for Airport ID badges must complete the badging process within thirty (30) calendar days of clearing their CHRC and STA.

(f) Any individual possessing an Airport ID badge must report to his or her supervisor or Authorized Signatory, within twenty-four (24) hours, if she or he has been convicted of, given a deferred sentence, found not guilty by reason of insanity or has been arrested and is awaiting judicial proceedings for any crimes listed in Title 49 CFR 1542.209. Airport Operator or Airport Operator sponsored employees and employees requesting Level 5 driving access must report this information in regard to any felony, as well as in regard to any of those crimes listed in Title 49 CFR 1542.209. The employee’s supervisor or Authorized Signatory must contact Airport Security within twenty-four (24) hours of being informed of such by his or her employee.

(g) Airport ID badge holders who are employees of the Airport Operator or Airport Operator sponsored companies may be required to resubmit fingerprints for an updated CHRC as part of the Airport’s ongoing random audit program.

20.04-7 Airport ID Badge Revalidation

(a) Airport ID badges expire on the date printed on the front of the badge, and may be revalidated up to thirty (30) calendar days prior to the expiration date.(b) For badge revalidation, the employee must complete and sign a Fingerprinting and Badging Application form, which has been signed by the employee’s Authorized Signatory no more than thirty (30) calendar days prior to the date the form is presented to Airport Security. The employee must also view the applicable training film(s) and pass the corresponding test(s) to assure understanding of the Denver Municipal Airport System Rules and Regulations. (c) If a Title 49 CFR Part 1542 Airport ID badge has been expired for thirty-one (31) days, the employee must also be fingerprinted, clear a CHRC, and have a valid STA before a badge can be reissued. (d) If a Title 49 CFR Part 1544 Airport ID badge has expired, the air carrier’s
Authorized Signatory must also certify the employee’s fingerprinting. A valid STA is required, as well, before a badge can be reissued.

20.04-8 Security Violation Notice Program and Appeals Process

(a) The Deputy Manager of Aviation – Airport Operations and his or her staff, DEN’s Contract Security Guard personnel and Denver Police Department (DPD) officers assigned to DEN may issue Violation Notices to Airport ID badge holders who fail to comply with this Part 20 and those Sections of Part 130 which have been deemed to be security-related. The issuance of a Violation Notice may result in the suspension or revocation of the Airport ID badge.

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

i) The pink copy will be given to the offender who is required to give the Violation Notice 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 to the offender’s authorized Signatory or Senior Company Manager. The two other copies will be sent to the appropriate Program Security Manager by the issuing agent.

ii) The Program Security Manager will send the white original via email and/or U.S. Mail to the Authorized Signatory or Senior Company Manager of the company for their follow up. A letter will be included informing the Authorized Signatory or Senior Company Manager of the follow up required.

iii) The file copy will be reviewed by the Program Security Manager, and pertinent information is entered into the Violation Notice computer tracking program.

iv) The Authorized Signatory or Senior Company Manager must ensure that the appropriate action is taken, either by completing the “Action Taken” section on the white copy and returning it via email and/or U.S. Mail to the Program Security Manager, or by contacting the Program Security Manager to set a hearing date, within ten (10) business days of the date of the letter. 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) Airport Security, serving on behalf of CCD reserves the right to deny, revoke or limit the scope of an individual’s Airport ID badge, endorsements or privileges based upon reasonable grounds and giving due consideration to the nature of the offense. Violations severe enough to require revocation under this Part 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, which does not require that a Violation Notice Hearing be held, he or she may, within ten (10) business days thereafter, make a written request for a meeting with the Program Security Manager, to review the facts giving rise to the Violation Notice. If such meeting is not requested, the Violation Notice will become valid, and the badge holder will have waived all rights to review or appeal thereof. If a meeting is timely requested, the Program Security Manager shall conduct an informal meeting with the person who was issued the Violation Notice. At the meeting, the Program Security Manager shall give the badge holder the opportunity to present facts and arguments as to why the Violation Notice was not properly issued, and shall consider the facts in support of the Violation Notice. The Program Security Manager 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 computer
tracking program.

(e) A Violation Notice Hearing, conducted by the Assistant Director of Security or designee will
be held when a Violation Notice is issued for a “Critical” violation, or when the holder of an
Airport ID badge is issued a second Violation Notice which is substantively the same as
another violation Notice issued to the same individual within a two (2) year period, or when
two (2) Violation Notices are issued to the badge holder for the same incident. A violation
Notice Hearing may be required for any Violation Notice issued, when the Program Security
Manager determines that the circumstances surrounding the issuance of the Violation Notice
indicate that a hearing is appropriate. A pre-hearing letter will be sent via email and/or U.S.
Mail informing the Authorized Signatory or Senior Company Manager that a Hearing must
be scheduled with Airport Security within ten (10) business days of the date of the letter, and
that a management representative or Authorized Signatory of the company/department must attend 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 the hearing, the Assistant Director of Security or designee determines that the
violation is valid, this will be communicated in writing to the Authorized Signatory of the
company/department , indicating the believed to have been committed by the 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 (f).

(f) 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
Director of Security will serve as the Appeals Officer. The Appeals Hearing shall be
conducted as expeditiously as possible, and in accordance with any rules adopted by the
Appeals Officer for such proceedings. All testimony and evidence shall be submitted under oath or affirmation. In all matters, the petitioner shall have the burden of proof to show by a
preponderance of the evidence the correctness of his or her position. The Appeals Officer shall
thereafter make a final written determination as to the action being appealed. A request for
reconsideration of the determination may be made if filed in writing with the Deputy
Manager of Aviation-Airport Operations within fifteen (15) calendar days of the date of
determination, or the final determination of the Appeals Officer may be reviewed under Rule 106(a)(4) of the Colorado Rules of Civil Procedure. If a request for reconsideration is made,
the Deputy Manager of Aviation- Airport Operations shall review the record, and issue a
written order concerning the reconsideration. The reconsideration determination shall be
considered a final order on behalf of the Manager of Aviation upon the date the
reconsideration determination is issued. The reconsideration determination shall be the final
order and may be reviewed under Rule 106(a)(4) of the Colorado Rules of Civil Procedure.

(g) 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 listed on the Violation Notice , and is attempting to be employed by a different
company, a management representative from the “new” company must attend the Violation
Notice Hearing with the employee.
20.04-9 Protection of Sensitive Security Information (SSI)
No participant of the Airport Security Program, and no Airport ID badge holder, shall divulge any security source documents or information 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 Title 49 CFR 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 key 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 key.
(b) All Airport ID badges and security keys shall be surrendered to Airport Security within ten (10) business days of the date when any employee or other individual to whom the badge or key(s) were issued terminates employment, is transferred to another location, or when the project or contract under which that individual was 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 keys issued to that individual may be suspended and no additional badges or security keys may be issued to that individual until the terminated badge or security keys 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 keys.

20.04-12 Display and Care of Airport ID Badge, Security Keys and Access Pin & Cipher Code Numbers
(a) All individuals in any area where an Airport ID badge is required must display the Airport ID Badge or other approved identification as defined in this Part on their persons at all times. 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 keys, any individual to whom such a badge and/or security key has been issued shall store his or her badge and/or security keys in a secure place in his or her possession and under his or her control at all times.
(c) Badge holders will not subject their Airport ID badges to extreme environmental elements.
(d) Any individual who is issued an access pin and/or cipher code number will ensure that it is kept in his or her immediate control to prevent unauthorized use and will ensure his or her access pin and/or cipher code number 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 keys 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 as to whether Airport Security will issue another Airport ID badge and/or security key to the individual.

20.04-13 Escorting in the Secured Area, Sterile Area and/or any Controlled Areas
(a) Escorting is only allowed by badge holders who hold escort authorized Airport ID badges.
(b) A badge holder who is authorized to perform escorts may escort only in those areas allowed by his or her access control profile.
(c) An escorting badge holder must keep individuals under his or her escort, in view and under control at all times.
(d) 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 managers (Assistant Aviation Operations Managers and above) may approve different escort ratios for special events.
(e) Escorting from a public area into the Secured Area is allowed only at designated access entry points. Escorting is not allowed at turnstile locations.
(f) Unbadged individuals may be escorted into the Secured Area up to three (3) times in one calendar year for official business only. Individuals who request Secured Area escorts more than three (3) times will be denied. Any request for an exception to this limit must be communicated in writing to the Airport Security Coordinator (ASC) for consideration prior to the time of the visit. This three (3) time limitation also applies to requests for Sterile Area Visitor ID badges. Differing escorting procedures at certain Airport perimeter facilities may apply.
(g) Unbadged individuals requesting access to, or badge holders who have no badge access to, a Controlled Area (e.g., the Airport Office Building) must be accompanied at all times while in the Controlled Area by an Airport ID badge holder who has badge access to the area.

20.04-14 Challenging and Reporting Unauthorized Persons
(a) Every Airport ID badge holder is responsible for challenging and/or reporting any individual in the Secured Area or any other Controlled Area, who is not properly displaying identification media as defined within this Part 20. An individual who does not challenge an apparently unauthorized person and is observed by Airport Security and/or TSA Inspectors may 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. DEN 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 Airport ID badge holder shall perform any of the following acts. The commission of any such
acts, due to their critical negative effect on the safety and security of Airport employees, the traveling public, and the national aviation system, is reason for immediate confiscation and suspension (and possible permanent revocation) of the Airport ID badge, issuance of a Violation Notice, and the requirement for a Violation Notice Hearing to be held, in accordance with Section 20.04-8:

(a) Loaning (or borrowing) the Airport ID badge or security key to anyone under any circumstances;
(b) Allowing unauthorized individuals or vehicles into the Secured Area, Sterile Area, and/or Controlled Areas;
(c) Blocking and/or damaging doors, gates, or card readers, and/or leaving doors or gates open that could be an access route into the Secured Area or Sterile Area for unauthorized individuals;
(d) Bypassing any portion or process of the security system;
(e) Altering the Airport ID badge;
(f) Interfering with or not complying with security screening, security procedures, and/or security personnel.

20.04-17 Civil Penalties Imposed by Transportation Security Administration (TSA)

(a) Any employer not regulated under Title 49 CFR Part 1544, Aircraft Operator, will be responsible for payment or reimbursement to the CCD of any civil penalties imposed by the TSA for individual security violations by their employees for violations under Title 49 CFR Part 1542.
(b) 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.
(c) If DEN is aware that an employee is under investigation by the TSA for individual security violations, the Airport ID badge may be suspended until the employee can provide Airport Security with formal documentation from TSA advising the investigation is complete and resolved.

20.05 Submission to Screening

20.05-1 No individual may enter the 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, with the following exceptions:
(a) Law Enforcement Officers (LEOs);
(b) TSA management and regulatory inspectors, as assigned by the DEN Federal Security Director;
(c) Those Airport ID badge holders with access to the AGTS train exits on Level 5 of the Jeppesen Terminal, who may use that access ONLY when alternative means of entry are not possible. Escorting is never allowed through this portal.

20.05-2 Pre-screened charter and scheduled operations are permitted direct access to a concourse in the Sterile Area if the screening of the individuals permitted such access by TSA is performed in a manner which has been approved by TSA.
20.06 Three-Foot Clear Zone
A clear zone of three (3) feet is established for both sides of all security fences around the Secured Area. The clear zone must not contain any object which could be of assistance to an individual trying to scale a fence.

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 all Airport ID badge holders to close and secure gates and doors in the terminal and concourse areas when not in use.

20.07-4 No Airport ID badge holder who is issued a security Personal Identification Number (PIN), and/or cipher code shall write or verbally announce in a public manner the number/code.

20.07-5 When an authorized Airport ID badge holder accesses a door, gate, or elevator leading to or from the Secured or Sterile Area, it is the badge holder’s responsibility to ensure that unauthorized individuals do not gain access to the Secured or Sterile Area.

20.07-6 When any Airport ID badge holder is in control of a door, gate, or elevator leading to or from the Secured or Sterile Area, it is the badge holder’s responsibility to ensure that unauthorized individuals or vehicles do not gain access to the Secured or Sterile Area. This applies to Airport ID badge holders who are physically located at the access point or who control an access point from a remote location. It also applies to Airport ID badge-holding bus drivers who allow passengers onto a bus which will enter the Secured Area.

20.07-7 Any Airport ID badge holder accessing either the Sterile or Secured Area through an access point requiring the use of biometrics (e.g., any turnstile location or any biometrically configured elevator) must comply with all restrictions regarding escorting through those locations, ensure that no tailgating is allowed, and ensure that any other badge holder also attempting to gain access through the location at the time uses the biometric device for access, as required.

20.07-8 When driving through a gate leading to or from the Secured 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 Secured 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 through the gate.

Denver Municipal Airport System Rules and Regulations
Source: Official Web site of Denver International Airport (business.flydenver.com)
20.07-9 When accessing or controlling a non-access control door, gate, or elevator leading to the Secured Area or Sterile 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 Secured Area or Sterile 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 personnel and/or contract security personnel arrive on scene and allow 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 personnel 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 door during the timed opening of the door. 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 through the door. The last individual to use the door by access control through which illegal entry occurred may 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 personnel 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.) providing entry to the Secured Area. No pedestrian traffic is allowed in the service tunnels.

20.07-12 All Airport ID badge holders whose badges do not allow a door disable function must obtain assistance from the Airport Communications Center to disable an access door.

20.07-13 All Airport ID badge holders in a vehicle entering a guarded security access gate which has an access control reader shall show their Airport ID badges to the guard on duty. Passengers in the vehicle without an Airport ID badge must show a government-issued picture ID and be entered into the escort program database (See 20.04-13(f) for number of times allowed). All Airport ID badges will be presented to the access control reader or compared to a stop list for validity verification. 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 Airport ID badge holder guarding a Secured Area or Sterile Area access point must display an Airport ID Badge, have a radio or telephone for emergency communications and have obtained instructions/permission from the Airport Communications Center.
20 AIRPORT SECURITY RULES AND REGULATIONS

20.07-15 When an Airport ID badge holder accesses a bag belt, it is the individual’s responsibility to ensure that unauthorized individuals are not allowed the opportunity to gain access to the Secured Area.

20.07-16 Any Airport ID badged employee controlling or operating a passenger loading bridge boarding door must use the access control reader for access before boarding passengers. If a passenger opens the door from the Secured Area and the door time open expires, the badged employee controlling the boarding may be issued a Violation Notice.

20.08 Use of Airport Federal Inspection Services (FIS) Facilities

20.08-1 All Airport ID badge holders in the FIS facilities during international flight processing must have an FIS seal displayed on their Airport ID badge, or be a CCD badged employee with a working demonstrated, work related need to be in the FIS facilities. Airport ID badge holders displaying an approved FIS seal are authorized to be in the FIS facilities ONLY during those times when there is a demonstrated, work-related need for them to be there.

20.08-2 No individual shall open a non-international access point door which would provide access out of the FIS Sterile Area during an international flight.

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

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 The FIS seal does not authorize escort privileges. An on-duty CBP Supervisor may authorize an escort if deemed appropriate.

20.08-6 Any individual who has no badge access to the FIS facilities must be escorted by CBP or Airport Operations personnel at all times while in the FIS facilities.

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

20.08-8 It is the employer’s responsibility to ensure all employees requiring access to the FIS facilities, or who work international flights, have FIS seals on their badges. The employer is also responsible for ensuring that all employees requiring badge access to international card readers on doors or bag belts (e.g., international customer service agents) have the required international job titles indicated on their badges.

20.08-9 All Airport ID badge holders who require an FIS seal must complete the CBP’s application process.

20.09 Actions or Conduct on Airport Property
Any Airport ID badge holder on DEN property whose actions and/or conduct may in any way affect the safety or security of the airport, the passengers or other Airport employees may have his or her Airport ID badge and/or security key(s) confiscated and suspended pending a hearing in accordance with Section

Denver Municipal Airport System Rules and Regulations
Source: Official Web site of Denver International Airport (business.flydenver.com)
20 AIRPORT SECURITY RULES AND REGULATIONS

20.04-8.

20.10 Weapons in the Secured Area and/or Sterile Area

20.10-1 Items as defined in the Denver Revised Municipal Code (www.denvergov.org) as well as any other item deemed a weapon by law enforcement authorities are forbidden to be possessed in the Secured Area, Sterile Area or any Controlled Area, without an approved, demonstrated need. Failure to comply with this regulation will result in a Violation Notice and may result in the suspension, confiscation and/or revocation of the individual’s Airport ID badge and/or security key(s) pending a hearing in accordance with Section 20.04-8.

20.10-2 All 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 Armed, on-duty Local, State and Federal Law Enforcement Officers on official business may be escorted into the Secured Area or any Controlled Area by an Airport ID badged Law Enforcement Officer.

20.11 Contraband in the Secured 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), as well as any other item deemed as contraband by local law enforcement authorities, are not allowed to be in or introduced to the Secured Area, Sterile Area, or any Controlled Area without an approved, demonstrated need.

20.12 Photography in the Sterile and Secured 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 Secured Areas is prohibited.

20.13 Unattended Baggage or Articles
Unattended baggage and/or articles are prohibited in all areas of DEN. 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.

20.14 Airport Vehicle Permits
(a) All vehicles operating in the Secured Area, with the exception of vehicles (e.g., baggage tugs) driven solely on Airport property and not required to be licensed by the State of Colorado, must display an Airport Vehicle Permit which is visible from the exterior of the vehicle.
(b) Airport Vehicle Permit 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 CCD.
(c) Airport Vehicle Permit requests are processed, reviewed and verified by Airport Security prior to their issuance.
(d) Airport Vehicle Permits may not be transferred between vehicles. Lost or stolen Airport Vehicle
Permits must be reported immediately to Airport Security.

**NOTICE**
The Rules and Regulations of the Denver Municipal Airport System are provided on the website of Denver International Airport, [www.flydenver.com](http://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](http://www.denvergov.org).

Revised Effective October 1, 2013