



DENVER INTERNATIONAL AIRPORT
TOGETHER WE SOAR



DENVER INTERNATIONAL AIRPORT | *Airport Security Privacy Policy*



Denver International Airport (“Airport Security”) respects your concerns about privacy and values our relationship with you. This Privacy Policy governs the personal information we obtain about badge applicants and badge holders who require access to Controlled, Secured, or Sterile Areas of the airport. To gain access to these Areas, companies must apply to become “Participants” in the Airport Security Program and individuals must receive an Airport ID badge.

This Privacy Policy describes the types of personal information we require to support the Airport Security Program, how we use that information, and how we, under certain conditions, disclose that information. This Privacy Policy also explains the measures we take to secure your personal information and the choices you have regarding our use of, and your ability to correct, the information.

I. What types of information does Airport Security collect?

The types of personal information we may obtain include:

Contact details (such as name, postal address, telephone number, and e-mail address);

Business contact information (such as employer’s name, job titles, business e-mail address, telephone number, Authorized Signatories and Senior Company Managers);

Physical characteristics (such as gender, height, and weight);

Government-issued identification information (such as a Social Security number and driver’s license, as well as copies of government-issued identification documents);

Digital photographs;

Biometric data (such as digital images of fingerprints);

Demographic details (such as date and place of birth, citizenship and work authorization status); and

Criminal background information

II. How does Airport Security collect your information?

We collect your personal information when:

Applicants fill out various Airport Security forms;

Receiving phone or electronic communication;

Physical or electronic documentation is provided to our office; and

Criminal History Records Checks (CHRCs) are received

III. Why does Airport Security collect your information?

Airport Security is responsible for issuing Airport ID badges, assigning and maintaining access to airport facilities, issuing vehicle permits, and verifying that badge applicants have cleared the required Security Threat Assessment (STA) and Criminal History Record Check (CHRC) prior to receiving their badge, and overall regulatory compliance with TSA Regulations and the Airport Security Program.

Individuals who require unescorted access to Controlled, Secured, or Sterile Areas must possess an Airport ID badge. To receive a badge, individuals must fill out the Fingerprinting & Badging Application and must also provide the necessary forms of identification or documentation. Visitors to the Controlled, Secured, or Sterile Areas may also be required to present limited Personally Identifiable Information (PII) before being allowed escorted or unescorted access.

Airport ID badge issuance is limited to those individuals who have cleared both the CHRC and STA and who have a frequent and recurring need for access. The Department of Homeland Security (DHS) uses the biographical information on your Fingerprinting & Badging Application to conduct the STA. Your fingerprint information is forwarded to the Federal Bureau of Investigation (FBI) for the CHRC. DHS will also transmit the fingerprints or enrollment into the US-VISIT’s Automated Biometrics Identification System (IDENT). If you provide your Social Security Number (SSN), DHS may provide your name and SSN to the Social Security

Administration (SSA) to ensure the validity of your name and SSN. This information may be shared with third parties during the course of a Security Threat Assessment, employment investigation, or adjudication of a waiver or appeal request to the extent necessary to obtain information pertinent to the assessment, investigation, or adjudication of your application or in accordance with the routine uses identified in the Transportation Security Threat Assessment System (T-STAS), DHS/TSA 002.

IV. Does Airport Security share your information?

Airport Security will not sell, rent or trade to third parties any personal information obtained from you except as disclosed in this Privacy Policy:

A. Biometric and Other Personal Information

We may disclose biometric data and other personal information for the purposes described in Section III of this Privacy Policy to airport authorities, the Transportation Security Administration (TSA), and other government authorities. Specifically, we may use biometric data and other personal information we obtain about Airport ID badge applicants and Airport Security Program Participants to:

Facilitate the Fingerprinting & Badging Application and enrollment process;

Administer the Airport Security Program; and

Verify applicants' and members' identities and conduct background checks and Security Threat Assessments concerning applicants

B. Non-Biometric Personal Information

We may also use personal information other than biometric data to:

Provide services to our badge applicants and Airport Security Program participants;

Respond to and communicate with our badge applicants and Airport Security Program participants about their questions and comments; and

Operate, evaluate, and improve our business (including analyzing our services and managing our communications)

C. Disclosures for Legal Compliance Purposes

Release of protected personal information may be prohibited under Local, State and Federal regulations such as C.R.S. § 24-72-204, 5 U.S.C § 552(b) and 49 U.S.C § 1520.

Finally, we may disclose information we obtain about badge applicants and Airport Security Program Participants if we are required to do so by law or pursuant to a legal process.

V. How does Airport Security protect your Personally Identifiable Information (PII)?

Airport Security takes your privacy very seriously. We take precautions to maintain the security, confidentiality, and integrity of the information that we collect. These precautions include access controls designed to limit access to the information to the extent necessary to accomplish our purposes. We also employ various security technologies to protect the information stored on our systems.

Disclosure of such information is limited to persons or entities under criteria identified in the Code of Federal Regulations, subject to a strict "need-to-know" standard, and as otherwise determined by the Transportation Security Administration (TSA) or the Department of Homeland Security (DHS).

The following are additional examples of security measures that we use to safeguard the personal information we maintain about our contractors:

Procedures for the identification and classification of personal information and implementation of safeguards appropriate to the sensitivity of the information;

Access control procedures designed to verify a security need before access to personal information is granted and procedures for the periodic review of access permissions;

Procedures for termination of access to personal information designed to curtail access to the information by terminated personnel or when there is no longer a need for access;

Personnel security controls designed to reduce the risk of human error, theft, fraud or misuse of facilities;

Physical security procedures designed to prevent unauthorized access, damage or interference to business premises and information; and

Technical controls to safeguard personal information, such as encryption, firewalls, and intrusion detection and prevention systems.

To make sure your personal information is secure, we communicate these guidelines to our employees and strictly enforce privacy safeguards within Denver International Airport (DIA).

VI. Can you access or correct your personal information?

Airport Security updates your Airport ID badge record with information that you provide on or with your Fingerprinting and Badging Application. You always have the right to review and submit corrections to the personal information you have provided. To correct your person information, you will need to submit a new Fingerprinting & Badging Application and provide supporting documentation for any name, citizenship, work authorization status or gender changes.

Updates to Our Privacy Policy

In light of increased security, this Privacy Policy is under continuous review and is subject to revision. Airport Security reserves the right to revise, amend, or modify this policy at any time and in any manner. When we change the policy in a material way, we will notify you through your company's Authorized Signatory.

Contact Us

If you have any questions about this Privacy Policy, please contact us at (303) 342-4300 or by email at airport.security@flydenver.com.