SAN DIEGO COUNTY REGIONAL AIRPORT AUTHORITY

POLICIES

ARTICLE 8 - GENERAL OPERATIONS
PART 8.6 - DOCUMENTS AND RECORDS
SECTION 8.63 - PRIVACY OF PERSONAL INFORMATION

PURPOSE: To establish a policy statement of the San Diego County Regional Airport Authority (the "Authority") for the prudent and reasonable protection of personal information ("PI") to the extent practicable.

POLICY STATEMENT:

(1) The Authority recognizes that privacy is a personal and fundamental right protected by Section 1 of Article I of the California Constitution, the U.S. Constitution, federal, state and local law. The Authority will not sell, lease or intentionally share PI in its possession with anyone else, except as follows:

(a) to the extent the Authority deems it necessary in furtherance of and for the purpose it was submitted;

(b) for use by an Authority employee acting solely in his or her official capacity;

(c) to help locate the owner of lost property;

(d) where required by applicable laws, including the California Public Records Act (Cal. Gov. Code § 6250 *et seq.*);

(e) where compelled by court order;

(f) where consented-to by the subject individual;

(g) where already in the public domain;

(h) where provided to the Authority on a public record or other record in furtherance of conducting business with the Authority (e.g., a meeting sign-in sheet or responses to requests for proposals, qualifications or bids); or

(i) in the course of an Authority or law enforcement investigation.

(2) In the event of any data breach of Authority records that includes PI, the Authority will make reasonable attempts to notify the owner(s) following discovery, where the PI was, or is reasonably believed to have been, accessed and/or acquired by an unauthorized person.

(3) Examples of Authority-protected PI elements include, but are not limited to:

(a) user name and password;
(b) full social security number;
(c) driver's license number;
(d) citizenship/legal status;
(e) race/ethnicity;
(f) birth date;
(g) home and personal cell telephone numbers;
(h) personal email address, mailing and home address;
(i) religious preference;
(j) security clearance;
(k) mother's middle and maiden names;
(l) family information: marital status, spouse information, child information, emergency contact information;
(m) biometric information;
(n) medical information;
(o) disability information;
(p) law enforcement records; and
(q) military records.

(4) Examples of PI elements not protected by the Authority include, but are not limited to:

(a) name and job description;
(b) office location; *
(c) office and work cell telephone numbers; *
(d) business e-mail address;
(e) information provided to the Authority on a meeting sign-in sheet or responses to requests for proposals, qualifications or bids; *
(f) badge number; and *
(g) salary, benefits and pension amounts.

(5) Prior to the intentional collection of PI from any person, the Authority will first disclose how such PI may be collected and used, and require the person's consent.

(6) The Authority shall retain PI in accordance with its Records Retention Policy.

(7) The Authority shall comply with all requirements of the California Civil Code relating to its use of any automated license plate recognition system.

* ***Except where disclosure is discretionary or would be in violation of local, state, or federal statues; or release of such information would potentially jeopardize the safety of the individual.***

[Adopted by Resolution No. 2015-0124 dated December 17, 2015.]