



REDMOND MUNICIPAL AIRPORT (RDM) Secured & Sterile Area ID Application

THIS PAGE FOR APPLICANT TO KEEP

Identification badges issued by Redmond Municipal Airport (RDM) are, and remain, property of the Airport. Badges must be returned immediately, the same day, under the following conditions:

- Upon separation of employment (for any reason)
- When job function no longer requires an Airport-issued identification badge
- Upon demand of the Airport
- Upon conviction of any of the disqualifying crimes listed in the application
- Upon expiration of “right to work” identification/documents.

ID's that are not returned to the RDM Airport as required are subject to a \$250.00 penalty, that may be assessed to either the individual the ID is issued to, or the company sponsoring the ID. This penalty is assessed at the discretion of the RDM Airport Security Coordinator.

Badges that are lost, stolen, or otherwise unaccounted for must be *immediately* reported by calling 541-504-3083 (no text messages).

Access to the Secured and/or Sterile Area is granted after undergoing a Federal Bureau of Investigation (FBI) fingerprint based Criminal History Records Check (CHRC) with no disqualifying offenses and the Transportation Security Administration's (TSA) Security Threat Analysis (STA) has deemed a favorable response. If favorable results are received, the applicant will be scheduled to attend a security training class to learn the responsibilities regarding access privileges to restricted areas of the Airport.

If a Criminal History Records Check (CHRC) performed by RDM results in disqualifying convictions, the applicant will be denied a security access ID. A copy of the CHRC will be provided if requested by the applicant in writing within 30 days for corrective purposes. If you have questions about the results of this CHRC, please contact Jayde Davis, RDM Airport Security Coordinator at 541-504-3090 or mail to Redmond Municipal Airport 2522 SE Jessie Butler Circle, #17, Redmond, OR 97756, attention Jayde Davis.

To schedule an Application Processing Appointment

please send email request to RDMID@flyrdm.com

Your I-9 ID documents will be reviewed, photo taken, fingerprints and completed application collected.

February 11, 2025



**REDMOND MUNICIPAL AIRPORT (RDM)
Secured & Sterile Area ID
Application**

AIRPORT USE - Date Received _____

Last Name (Sr. Jr. I II) **Legal First Name** **Full Middle Name**

REQUIRED - Social Security Number _____

LIST ALL - COMMON NAME, NICK NAMES / FORMER NAMES / ALIAS:

LAST NAME FIRST NAME MIDDLE NAME

LAST NAME FIRST NAME MIDDLE NAME

LAST NAME FIRST NAME MIDDLE NAME

Mailing Address _____

City State Zip

Main Phone _____ **Alternate phone** _____

Email Address _____

Date of Birth _____ **State & City of Birth** _____

CITIZENSHIP COUNTRY _____ **Gender** Male Female

Race Asian Black White Latino Native American Other

Eye Color _____ **Hair Color** _____ **Height** _____ **Weight** _____

CHECK THIS BOX IF YOU INTEND TO OPERATE AS A SASO (SPECIALIZED AVIATION SERVICE OPERATOR) AT RDM. A SASO IS DEFINED ANY COMMERCIAL AERONAUTICAL SERVICE PROVIDER THAT PROVIDES ANY ONE OR A COMBINATION OF THE FOLLOWING ACTIVITIES: FLIGHT TRAINING, AIRFRAME AND POWERPLANT MAINTENANCE, AVIONICS SALES AND MAINTENANCE, AIRCRAFT RENTAL, AIRCRAFT CHARTER OR TAXI, AIRCRAFT MANAGEMENT, AIRCRAFT STORAGE HANGARS, AIRCRAFT SALES, AIRCRAFT RESTORATION AND REFURBISHING, AND SPECIALIZED AIRCRAFT SERVICES. PLEASE NOTE: INDIVIDUALS OR ENTITIES OPERATING AS A SASO AT RDM ARE REQUIRED TO UNDERGO ADDITIONAL APPLICATION AND PERMIT REQUIREMENTS PRIOR TO OBTAINING AN RDM ID.

Employer / Company Name _____

Manager or Supervisor Name _____

Emergency Contact Name _____ **Relationship:** _____

Main Phone _____ **Alternate Phone** _____

I understand that my RDM ID is a highly accountable item, and remains property of the RDM Airport. I understand if I do not return my ID to the RDM Airport as required, I may be assessed a \$250.00 penalty:

Signature

Date

February 11, 2025

TSA Privacy Act Statement

Authority: 6 U.S.C. § 1140, 46 U.S.C. § 70105; 49 U.S.C. §§ 106, 114, 5103a, 40103(b)(3), 40113, 44903, 44935-44936, 44939, and 46105; the Implementing Recommendations of the 9/11 Commission Act of 2007, § 1520 (121 Stat. 444, Public Law 110-53, August 3, 2007); FAA Reauthorization Act of 2018, §1934(c) (132 Stat. 3186, Public Law 115-254, Oct 5, 2018), and Executive Order 9397 (November 22, 1943), as amended.

Purpose: The Department of Homeland Security (DHS) will use the information to conduct a security threat assessment. If applicable, your fingerprints and associated information will be provided to the Federal Bureau of Investigation (FBI) for the purpose of comparing your fingerprints to other fingerprints in the FBI's Next Generation Identification (NGI) system or its successor systems including civil, criminal, and latent fingerprint repositories. The FBI may retain your fingerprints and associated information in NGI after the completion of this application and, while retained, your fingerprints may continue to be compared against other fingerprints submitted to or retained by NGI. DHS will also transmit your fingerprints for enrollment into US-VISIT Automated Biometrics Identification System (IDENT). DHS will also maintain a national, centralized revocation database of individuals who have had airport- or aircraft operator- issued identification media revoked for noncompliance with aviation security requirements. DHS has established a process to allow an individual whose name is mistakenly entered into the database to correct the record and have the individual's name expunged from the database. If an individual who is listed in the centralized database wishes to pursue expungement due to mistaken identity, the individual must send an email to TSA at Aviation.workers@tsa.dhs.gov.

Routine Uses: In addition to those disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. § 552a(b)(3) including 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 TSA system of records notice (SORN) DHS/TSA 002, Transportation Security Threat Assessment System. For as long as your fingerprints and associated information are retained in NGI, your information may be disclosed pursuant to your consent or without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses.

Disclosure: Pursuant to § 1934(c) of the FAA Reauthorization Act of 2018, TSA is required to collect your SSN on applications for Secure Identification Display Area (SIDA) credentials. For SIDA applications, failure to provide this information will result in denial of a credential. For other aviation credentials, although furnishing your SSN is voluntary, if you do not provide the information requested, DHS may be unable to complete your security threat assessment.

Additional Notices and Disclosures

Screening Notice: Any employee holding a credential (RDM issued ID) granting access to a Security Identification Display Area (SIDA) may be screened at any time while gaining access to, working in, or leaving a Security Identification Display Area (SIDA). The screening may include any and all items in that individual's possession at the time of screening.

CRD Notice: Pursuant to TSA-NA-21-01 series, RDM will utilize the Centralized Revocation Database (CRD) as applicable, to report permanently revoked RDM ID media due to an ID holder's failure to comply with security requirements. RDM will grant ID holders 7 calendar days to appeal a revocation prior to entering their information into the CRD. If the individual does not appeal the revocation of the ID within 7 business days of notification of the intent to revoke ID, or the decision to revoke is upheld following the appeal, RDM will record the revocation in the CRD utilizing the FPRD system within 3 calendar days.

Continued on next page...

February 11, 2025

RDM ID Application
Additional Notices and Disclosures Continued
& CFR Part 1540 Certification Page

RDM will review any available information in the CRD for all applicants for Secured or Sterile Area ID's, and will consider the information provided when determining an individual's eligibility to receive an RDM ID.

Badge holders not subject to entry into the CRD include: RDM AOA ID holders, employees of Federal, State or local government (including law enforcement officers), who as a condition of employment, have been subjected to an employment investigation that includes a CHRC; direct employees of, and Transportation Security Officers under contract to the TSA, Federal Aviation Administration, or Customs and Border Protection; and employees of the U.S. Department of Defense (DOD) operating within exclusive areas of a regulated airport.

The information I have provided is true, complete, and correct to the best of my knowledge and belief and is provided in good faith. I understand that a knowing and willful false statement can be punished by fine or imprisonment or both (see Section 1001 of Title 18 of the United States Code).

I authorize the Social Security Administration to release my Social Security Number and full name to the Transportation Security Administration, Enrollment Services and Vetting Programs, Attention: Vetting Programs (TSA-10)/Aviation Worker Program, 6595 Springfield Center Drive, Springfield, VA 20598-6010.

I am the individual to whom the information applies and want this information released to verify that my SSN is correct. I know that if I make any representation that I know is false to obtain information from Social Security records, I could be punished by a fine or imprisonment or both.

Code of Federal Regulation (CFR)
PART 1540—CIVIL AVIATION SECURITY: GENERAL RULES

Subpart B—Responsibilities of Passengers and Other Individuals and Persons

§1540.105 Security responsibilities of employees and other persons.

(a) No person may:

(1) Tamper or interfere with, compromise, modify, attempt to circumvent, or cause a person to tamper or interfere with, compromise, modify, or attempt to circumvent any security system, measure, or procedure implemented under this subchapter.

(2) Enter, or be present within, a secured area, Airport Operations Area (AOA), Security Identification Display Area (SIDA) or sterile area without complying with the systems, measures, or procedures being applied to control access to, or presence or movement in, such areas.

(3) Use, allow to be used, or cause to be used, any airport-issued or airport-approved access medium or identification medium that authorizes the access, presence, or movement of persons or vehicles in Secured Areas, Airport Operations Area AOA's, or Security Identification Display Areas (SIDAs) in any other manner than that for which it was issued by the appropriate authority under this subchapter.

I attest, as an applicant for RDM issued ID, and/or key(s), and/or electronic access device, that I understand my security responsibilities under the above CFR, 49 CFR 1540.105(a), and acknowledge receipt of the TSA Privacy Act Statement.

Signature: _____

Date of Birth (Month / Day / Year) : _____

SSN and Full Name printed: _____

February 11, 2025

Criminal History Record Check - CHRC

Please Note: Each box must be individually marked

Have you been convicted or found not guilty by reason of insanity of any of the following in the past ten (10) years?

Yes No

- Forgery of certificates, false marking of aircraft, and other aircraft registration violation; 49 U.S.C.46306 interference with air navigation; 49 U.S.C.46308
- Improper transportation of a hazardous material; 49 U.S.C.46312
- Aircraft piracy; 49 U.S.C.46502
- Interference with flight crew members or flight attendants; 49 U.S.C.46504
- Commission of certain crimes aboard aircraft in flight; 49 U.S.C.46506
- Carrying a weapon or explosive aboard aircraft; 49 U.S.C.46505
- Conveying false information and threats; 49 U.S.C.46507
- Aircraft piracy outside the special aircraft jurisdiction of the United States; 49 U.S.C.46502 (b)
- Lighting violations involving transporting controlled substances; 49 U.S.C.46315
- Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements; 49 U.S.C.46314
- Destruction of an aircraft or aircraft facility; 18 U.S.C.32
- Murder
- Assault with intent to murder
- Espionage
- Sedition
- Kidnapping or hostage taking
- Treason
- Rape or aggravated sexual abuse
- Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon
- Extortion
- Armed or felony unarmed robbery
- Distribution of, or intent to distribute, a controlled substance
- Felony arson
- Felony involving a threat
- Felony involving:
 - Willful destruction of property;
 - Importation or manufacture of a controlled substance;
 - Burglary;
 - Theft;
 - Dishonesty, fraud, or misrepresentation;
 - Possession or distribution of stolen property;
 - Aggravated assault;
 - Bribery; or
 - Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than 1 year.

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

Conspiracy or attempt to commit any of the criminal acts listed in this paragraph.

I understand my signature below reflects that I do not have a disqualifying criminal offense. Federal Regulations under 49 CFR 1542.209 (1) imposes a continuing obligation to disclose to the airport operator within 24 hours if you have been convicted of any disqualifying criminal offense that occurs while you have unescorted access authority. The information I have provided on this application is true, complete, and correct to the best of my knowledge and belief and is provided in good faith. I understand that a knowing and willful false statement on this application can be punished by fine or imprisonment or both. (See section 1001 of Title 18 United States Code.)

Signature _____ Date _____

Name (print legibly) _____

February 11, 2025



Redmond Municipal Airport (RDM) Employee Parking Lot Rules

INSTRUCTIONS: *Keep this page for your reference. Sign the second page, return to the Airport Badging Office.*

1. **Access to the Employee Parking Lot is ONLY for Airport authorized use. You are NOT permitted to loan your Airport Secured or Sterile Area ID or parking card to anyone for ANY reason. You are NOT authorized to grant access to the employee lot to other individuals using YOUR Airport ID or parking card, no exceptions.** Please refer individuals needing assistance to Airport Administration or Security Offices, or on-site security officer for assistance.
 - Allowing individuals access to the employee parking lot may result in **your** parking privileges being permanently revoked and may also result in a TSA violation leading to civil penalties.
2. **Employee parking privileges are for business and employment purposes ONLY; personal or leisure use is not permitted.**
 - Unauthorized use or access to employee parking may result in fines and permanent loss of parking privileges.
3. Employee must park in Airport authorized assigned locations within the parking lot.
4. Overnight / Multi-day parking in the employee lot is only authorized for business travel purposes when pre-authorized by your employer.
 - Your manager will provide an overnight permit that must be displayed on the Driver's side dashboard and you must park your vehicle in the designated Transient parking area to avoid receiving a \$50.00 citation.
5. Parking within Rental Car Lot or Rental Car Overflow Lot by employees is strictly prohibited!
6. Motorcycles for must be registered with Airport Administration – to register your motorcycle, please call (541) 504-3084. Motorcycles must be parked within the Airport's designated motorcycle parking area.
 - Motorcycles are NOT authorized to parking in the employee lot since the gate arm may cause injury and/or damage.
7. During winter weather months, do not back into parking spaces that have adjacent sidewalks.
 - Vehicles that are backed-in often prohibits effective snow removal from sidewalks, and may be cited.
8. Do not litter, this includes trash, food, and cigarette butts.
 - Food and other litter attract birds, birds and aircraft NEVER mix.
 - A covered garbage can is available for use in the employee parking lot.
9. Be extremely mindful and cautious of pedestrians while also observing the posted speed limits (15 MPH).
10. If you are receiving a temporary parking card, it must be returned. You will need to return it to the Airport Badging Office **prior** to being issued a permanent RDM ID.
 - If the hiring process is stopped by either party prior to receiving an ID, you must **immediately** return the parking card, or you may be charged a \$100.00 lost fee.
 - The Airport may send unpaid lost fee to collections, which significantly increases the total amount owed.
11. **Test your parking card** at the employee gate **prior** to leaving the Airport to ensure it works for you; if the card is not working, call the badging office at (541) 504-3088.
12. When exiting, slowly get close to gate, it will open to allow exit (no card needed).

Card Reader Instructions:

1. Hold the parking card flat against (touching) the card reader; the reader will 'beep' and the light bar at the top will flash different colors (you may need to put hand over the color bar at the top of reader to see this if it is bright outside).
2. Remove the card from the reader so it does not continue to re-scan continuously.
3. Enter the PIN number (last 4 of your Social Security Number, unless otherwise indicated when issued); no special characters are required. If entered correctly, the reader will flash green and the gate will open.
4. If the card reader flashes red at any step:
 - Wait 10 seconds, try the process again.
 - After two or three attempts, there may be a problem with the card; bring your parking card to the Airport Badging Office for assistance.
 - Parking is not validated for individuals that do not test their parking cards immediately after issuance.

February 11, 2025



Redmond Municipal Airport (RDM) Employee Parking Lot Rules

ACKNOWLEDGMENT OF RDM AIRPORT EMPLOYEE PARKING LOT RULES

Notwithstanding anything contained in this Agreement to the contrary, City makes no representations, warranties, and/or covenants concerning the Parking Area and/or Permittee’s use of the Parking Area. City will not monitor and/or provide any security for or concerning the Parking Area. Permittee acknowledges and agrees that (a) theft, damage, destruction, and/or loss may occur to Permittee’s vehicle(s) and/or contents located therein while the vehicle(s) are operated and/or parked in the Parking Area, and (b) City is not liable or responsible for any theft, damage, destruction, and/or loss to Permittee’s vehicle(s) and/or contents located therein. Permittee assumes all risk associated with Permittee’s use of the Parking Area, including, without limitation, theft, damage, destruction, and/or loss to Permittee’s property (e.g., vehicle damage and/or theft). Permittee accepts the Parking Area on an “AS-IS” “WHERE-IS” AND “WITH ALL FAULTS” basis. Permittee’s use of the Parking Area may be disrupted by certain expansion, improvement, construction, development, maintenance, repairs, and/or other activities on or at the Parking Area. Permittee will have no claim and/or cause of action against City if Permittee is disrupted in the use of the Parking Area due to the aforementioned activities.

I, the undersigned, attest I have received, understand and agree to abide by Airport employee parking rules. I have received employee parking privileges via an Airport issued parking card, or Secured or Sterile Area ID. I understand that I am the only person authorized to use the parking card or ID and authorized to use my parking card or ID for my vehicle only, no exceptions. I am not authorized to use my parking card or ID to allow access for others to enter the employee parking lot. If I allow any other person access to the employee parking lot, I could permanently lose employee parking privileges and be subject to TSA civil penalties. I understand employee parking privileges are for employment purposes only. **Personal use of the employee parking lot is NOT permitted.**

I understand I **must return the parking card** to the Airport Badging Office, otherwise I may be charged the \$100.00 lost fee.

Date _____

Printed Name _____

Signature _____

Employer _____

February 11, 2025

LISTS OF ACCEPTABLE DOCUMENTS - Documents must be UNEXPIRED

ONE selection from List A

OR a combination of ONE from List B **AND** ONE from List C.

LIST A ONE ID ONLY OR ONE ID FROM LIST B AND ONE ID FROM LIST C

LIST A Documents that Establish Both Identity and Employment Authorization	OR	LIST B Documents that Establish Identity	LIST C Documents that Establish Employment Authorization
<ol style="list-style-type: none"> 1. U.S. Passport or U.S. Passport Card 2. Permanent Resident Card or Alien Registration Receipt Card (Form I-551) 3. Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa 4. Employment Authorization Document that contains a photograph (Form I-766) 5. For a nonimmigrant alien authorized to work for a specific employer because of his or her status: <ol style="list-style-type: none"> a. Foreign passport; and b. Form I-94 or Form I-94A that has the following: <ol style="list-style-type: none"> (1) The same name as the passport; and (2) An endorsement of the alien's nonimmigrant status as long as that period of endorsement has not yet expired and the proposed employment is not in conflict with any restrictions or limitations identified on the form. 6. Passport from the Federated States of Micronesia (FSM) or the Republic of the Marshall Islands (RMI) with Form I-94 or Form I-94A indicating nonimmigrant admission under the Compact of Free Association Between the United States and the FSM or RMI 	AND	<ol style="list-style-type: none"> 1. Driver's license or ID card issued by a State or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address 2. ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address 3. School ID card with a photograph 4. Voter's registration card 5. U.S. Military card or draft record 6. Military dependent's ID card 7. U.S. Coast Guard Merchant Mariner Card 8. Native American tribal document 9. Driver's license issued by a Canadian government authority <p style="text-align: center;">For persons under age 18 who are unable to present a document listed above:</p> <ol style="list-style-type: none"> 10. School record or report card 11. Clinic, doctor, or hospital record 12. Day-care or nursery school record 	<ol style="list-style-type: none"> 1. A Social Security Account Number card, unless the card includes one of the following restrictions: <ol style="list-style-type: none"> (1) NOT VALID FOR EMPLOYMENT (2) VALID FOR WORK ONLY WITH INS AUTHORIZATION (3) VALID FOR WORK ONLY WITH DHS AUTHORIZATION 2. Certification of Birth Abroad issued by the Department of State (Form FS-545) 3. Certification of Report of Birth issued by the Department of State (Form DS-1350) 4. Original or certified copy of birth certificate issued by a State, county, municipal authority, or territory of the United States bearing an official seal 5. Native American tribal document 6. U.S. Citizen ID Card (Form I-197) 7. Identification Card for Use of Resident Citizen in the United States (Form I-179) 8. Employment authorization document issued by the Department of Homeland Security

*****NOTE: CONCEAL CARRY LICENSE / PERMIT is NOT an acceptable I-9 ID**