Melbourne Orlando International Airport

Security Identification Badge Application
MAA Badge Office: 321-409-2192 ~ Application available at www.mlbairportbadging.com

The Melbourne Airport Authority (MAA) will not accept this application if it is not legible, altered (including use of correction fluid), torn, folded, bent or otherwise defaced. The application must be completed in the presence of your authorized signatory. Signatures by the employee and authorized signatory will only be accepted using blue ink. The application must be processed within two weeks of the date it is signed by the authorized signatory.

This application must be printed in color.

SECTION 1 - APPLICANT INFORMATION: Handprinted forms must be in CAPTIAL LETTERS

Present this application with the proper forms of identification from the List of Acceptable Documents. All documents must be original and unexpired.

LAST NAME	FIRST NAME	MIDDLE NAME
LIST ANY AND ALL OTHER LEGAL NAME(S) PREVIOUSLY USED (i.e. maiden name)		EMAIL ADDRESS

HOME ADDRESS	CITY	STATE	ZIP CODE

HOME PHONE NUMBER	CELL PHONE NUMBER	WORK PHONE NUMBER

DATE OF BIRTH (mm/dd/yyyy)	U.S. SOCIAL SECURITY NUMBER	GENDER	RACE	EYE COLOR	HAIR COLOR	HEIGHT	WEIGHT
/ /	- -	☐ MALE ☐ FEMALE				ft in	lbs

NAME OF AIRPORT SPONSOR (Employer & Job Title or Tenant/Hangar #)	DRIVER'S LICENSE NUMBER	LICENSE STATE	LICENSE EXPIRATION DATE
			/ /

SECTION 2 - CITIZENSHIP INFORMATION

Mark appropriate boxes below and answer any relevant questions.

COUNTRY OF BIRTH: _____

COUNTRY OF CITIZENSHIP: _____

☐ US CITIZEN BORN WITHIN THE US OR ITS TERRITORIES

STATE OF BIRTH: _____

☐ NON-US CITIZEN
Must provide at least ONE of the following ORIGINAL and UNEXPIRED documents:

ALIEN REGISTRATION NUMBER (ARN): _____

I-94 ARRIVAL/DEPARTURE FORM NUMBER: _____

☐ OTHER US CITIZEN NATURALIZED OR BORN ABROAD
Must provide one of the following ORIGINAL and UNEXPIRED documents:

US PASSPORT NUMBER: _____

CERT. OF NATURALIZATION NUMBER (ARN OR INS): _____

CERT. OF BIRTH ABROAD (FORM DS-1350): _____

☐ NON-IMMIGRANT VISA HOLDER
Must provide the following ORIGINAL and UNEXPIRED documents:

NON-IMMIGRANT VISA CONTROL NUMBER: _____

PASSPORT NUMBER: _____

PASSPORT ISSUING COUNTRY: _____

SECTION 3 – DISQUALIFYING CRIMINAL OFFENSES

This section must be completed by the applicant from Section 1.
Applicant must mark the appropriate statement at the bottom of the section.

Please read the following information carefully. Indicate below if you have been convicted, given a deferred sentence, found not guilty by reason of insanity or been arrested and awaiting judicial proceedings. A conviction for any offense (even a misdemeanor offense) listed in 49 CFR 1542.209 will disqualify an individual from receiving a MAA security identification badge.

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.
Felony involving importation or manufacture of a controlled substance.
Felony involving burglary.
Felony involving theft.
Felony involving dishonesty, fraud, or misrepresentation.
Felony involving possession or distribution of stolen property.
Felony involving aggravated assault.
Felony involving bribery.
Felony involving 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 (d).

ALL APPLICANTS MUST MARK EITHER YES OR NO TO THE STATEMENT BELOW.

☐ Yes – I have been convicted, given a deferred sentence, found not guilty by reason of insanity or been arrested and awaiting judicial proceedings of ANY of the disqualifying criminal offenses listed above within the last 10 years.

☐ No – I have NOT been convicted, given a deferred sentence, found not guilty by reason of insanity or been arrested and awaiting judicial proceedings of ANY of the disqualifying criminal offenses listed above within the last 10 years.

NOTE: A copy of the criminal record received from the FBI will be provided to you upon receipt of a written request to the Airport Security Coordinator (ASC).
Direct all questions about the results of the CHRC to: Airport Security Coordinator, Melbourne Orlando International Airport, 1 Air Terminal Parkway, Melbourne, FL 32901

AIRPORT BADGE OFFICE USE ONLY

Issue Date:	Color:	Badge #:	Encoded Card #:	Emp. Code:	Exp. Date:	Pin #:	Ramp Date:

Airport Security Coordinator Signature:	Date:

THIS APPLICATION MUST BE PRINTED IN COLOR

REV. SEP. 2021

SECTION 4 – PRIVACY ACT NOTICE STATEMENT

Read this section in its entirety.
Applicant must print, sign and date at the bottom of the section.

The Privacy Act of 1974 - 5 U.S.C. 552a(e)(3)
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), 40.113, 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.
I acknowledge that I am aware that the collection of information is required for the above reasons and I have received a copy of the DHS Privacy Act Notice.

Printed Name _____ Signature (Blue Ink Only) _____ Date _____

SECTION 5 – APPLICANT AGREEMENT SECTION

Carefully read this section. Applicant from Section 1 must complete the bottom of the section.

Prior to issuance of a MAA security identification badge the Department of Homeland Security (DHS), the Transportation Security Administration (TSA), and the Melbourne Airport Authority (MAA) requires all individuals that request unescorted access to the Air Operations Area (AOA), Security Identification Display Area (SIDA), and/or Sterile Areas must submit to and pass a fingerprint-based Criminal History Records Check (CHRC) and Security Threat Assessment (STA) to be in compliance with 49 CFR 1542 and the MAA Rules and Regulations. I acknowledge that Federal regulations under 49 CFR Part 1542.209(l) impose a continuing obligation to disclose to MAA within twenty-four hours if I am convicted or found not guilty by reason of insanity any Disqualifying Criminal Offenses (Section 3) that occur while I have unescorted access authority. If arrested for any of these offenses I acknowledge that I am responsible for notifying the airport within twenty-four hours of the arrest. MAA reserves the right to deny a badge application for any reason. All badges remain the property of the MAA and must be surrendered upon demand or returned to the MAA upon the individual's termination of employment or work assignment at the Melbourne Orlando International Airport. I release MAA from liability whatsoever in connection with the CHRC with regards to my request for the issuance of a MAA security identification badge. -By signing below, I certify, acknowledge receipt and have read the "Melbourne Orlando International Security Identification Badge Rules and Regulations" (see attached) from the MAA Badge Office and agree to comply with and abide by all applicable Federal, State, local, and MAA rules, regulations, laws, ordinances, and training received. 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 fully acknowledge my security responsibilities as outlined in TSR 1540.105(a) – Security Responsibilities of Employees and other Persons and will comply with all airport security rules. I further acknowledge that I may lose my access privileges or be subject to civil penalties for violating these rules. Social Security Administration Verification: I authorize the Social Security Administration to release my Social Security Number and full name to the Transportation Security Administration, Enrollments 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. I acknowledge holding a credential granting access to a Security Identification Display Area may cause me to be screened at any time while gaining access to, working in, or leaving the Security Identification Display Area.

☐ (CHECK BOX) By signature below; I acknowledge and understand my responsibilities under 49 CFR 1540.105(a) as a MAA badge holder who is being allowed escort authority privileges.

Print Full Name _____ DATE OF BIRTH (mm/dd/yyyy) ___/___/___

Signature (Blue Ink Only) _____ SOCIAL SECURITY NUMBER ___-___-___

SECTION 6 – AUTHORIZED SIGNATORY SECTION

Prior to completion of this section, the Authorized Signatory must validate information provided by the Applicant in Sections 1-5.

TYPE OF MEDIA REQUESTED (Check all that apply) ☐ AOA ☐ SIDA ☐ Renewal ☐ LEO - Armed ☐ Replacement for Lost/Stolen Badge ☐ GA Badge	ESCORT PRIVILEGES REQUIRED ☐ YES ☐ NO ☐ If YES, (CHECK BOX) I attest that a *specific need exists for providing the individual applicant with unescorted access authority.*
DRIVING PRIVILEGES REQUIRED ☐ None ☐ Non-Movement Area (Ramps/Aprons Only) ☐ Movement Area (Runways/Taxiways)	KEYS REQUIRED ☐ None ☐ Yes If Yes, list key #'s needed _____
VERIFIED APPLICANTS CITIZENSHIP & ID'S ☐ Yes, I as Authorized Signatory have personally verified this badge applicant's acceptable forms of ID's	CBP AREA REQUESTED (Additional Forms Required) ☐ None ☐ Zone 1 ☐ Zone 2 ☐ Zone 1 & 2
NOTES:	

My signature below certifies: I have reviewed this application for accuracy and request the named employee/applicant be fingerprinted and apply for the media type indicated above. That all conditions of TSA regulations 49 CFR, parts 1540, 1542, 1544 and 1546 have been met. I attest that a specific need exists for providing the individual applicant with unescorted access authority and the individual applicant acknowledges their security responsibilities under 49 CFR 1540.105(a). I am aware of and will comply with all the rules and procedures set forth in the required annual Signatory Authority Training (SAT) and the MAA Security Identification Badge Rules and Regulations. Failure to follow these rules, regulations and procedures will subject myself as the authorized signatory, the company I represent, and/or the badge holder to possible penalties and fines. I am aware that a fee will be imposed for lost, misplaced or stolen badges and that I must immediately report to the MAA Badge Office any lost/stolen media. I will immediately notify the MAA Badge Office of any badge applicants or badge holders that have been terminated or separated and will return all badges and/or keys to the MAA Badge Office within 24 business hours. The information I have provided is true, correct, and complete to the best of my knowledge and belief. I acknowledge that a knowing and willful false statement can be punished by fine or imprisonment or both (Section 1001 of Title 18 of the United States Code).

SPONSOR'S PRINTED NAME	SPONSOR'S COMPANY	SAT TRAINING DATE	PHONE NUMBER	E-MAIL ADDRESS

SIGNATURE (Blue Ink Only)	DATE (Application Expires 2 Weeks From This Date)

THIS APPLICATION MUST BE PRINTED IN COLOR

Melbourne Orlando International Airport
Security Identification Badge Rules and Regulations

APPLICANT MUST RETAIN THESE RULES AND REGULATIONS

1. MAA security identification badge applications are required for issuance of new or renewal MAA security identification badges. Applicants must read, complete and sign all applicable areas of the application in the presence of their authorized signatories before submitting application to the MAA Badge Office. There is a $77 fee for new badges and a $37 fee for renewals.
2. Once the authorized signatory signs and dates the MAA security identification badge application you have two weeks to present the completed application and acceptable forms of identification to the MAA Badge Office. No faxes or scanned copies of the application or your identification will be accepted.
3. The U.S. Department of Homeland Security (DHS) and the Transportation Security Administration (TSA) requires that all individuals that request unescorted access to the secured areas of the airport must submit to and pass a Security Threat Assessment (STA) and a fingerprint-based Criminal History Records Check (CHRC).
4. Individuals applying for unescorted access to the Sterile or Secure areas of the airport must attend a Security Identification Display Area (SIDA) training class.
5. All applicants must submit proof of identity, citizenship status and/or legal employment status. Acceptable forms of IDs are listed in the USCIS Form I-9 attached. If applicant was born outside the U.S. and are now a citizen, they must present a current/unexpired U.S. passport, a certified copy of their Certificate of Citizenship, Certificate of Naturalization, or a Certification of Birth from Abroad (form DS 1350, FS-240, or FS-545). These documents will be presented at the time applications and fingerprints are to be completed.
6. I agree to comply at all times with the MAA Rules and Regulations, and the provisions of Title 49, CFR, Parts 1540, 1542, and 1544.
7. All persons in the SIDA, Secured Areas, and Air Operations Area (AOA) portion of MAA will be required to display on their persons, at all times, the properly issued MAA security identification badge. The MAA security identification badge will be displayed on the upper portion of the body on the outer garment so as to be clearly visible.
8. It is the responsibility of each MAA security identification badge holder to challenge any individual not displaying their MAA security identification badge while on Airport property.
   Challenge procedures are:
   - Approach the un-badged individual in a non-threatening and helpful manner and inquire as to the reasons why the un-badged individual is within the secure area portion of the Airport.
   - When an un-badged individual cannot produce an MAA security identification badge, the individual conducting the challenge must escort the person out of the secure area and immediately report this incident to a Melbourne International Airport Police Officer for further investigation.
   - If an authorized individual cannot approach an un-badged person for safety reasons, the authorized individual must keep close surveillance of the un-badged person and immediately contact a Melbourne International Airport Police Officer to report the incident.
   - The 24 hour Melbourne International Airport Police Department (MAPD) emergency notification number is 321-288-0147, which is located on the back of the MAA security identification badge.
9. The MAA security identification badge must be produced if asked to be verified by TSA, law enforcement, Airport staff or authorized badge holders. If a MAA Security badge holder does not have their badge at the time of verification, they will be escorted out of the restricted area and not allowed access until they can produce their MAA security identification badge.
10. Each person must enter AOA, SIDA/Secure, and Sterile Area using their issued MAA security identification badge. Multiple persons entering an automated access point on a single entry transaction is PROHIBITED. The only exceptions are the electric eyes on the ramp where all vehicle occupants must process their MAA security identification badge on the reader. Each badge holder must swipe their badge and wait for the door to securely close before the next person swipes their badge. All badge holders shall wait until the door or gate is fully closed before leaving the area.
11. If an alarm is activated, the individual must remain in the area and immediately contact the MAPD.
12. Employees traveling as passengers must access the sterile area through a TSA screening checkpoint with any accessible property they intend to carry onboard the aircraft and must remain in the sterile area after entering. This requirement applies when traveling for all purposes (business, leisure, etc.) unless exempt by federal regulation.
13. The MAA security identification badge is issued to support my job duties and responsibilities at the airport and should only be used for official business purposes. I will never utilize the MAA security identification badge for personal or off-duty use. Never put MAA security identification badges on any social media.
14. It is not permissible, under any circumstances, to use another person's MAA security identification badge or to allow another person to use your MAA security identification badge.
15. Keys are only issued to individuals that possess valid MAA security identification badges.
16. MAA security identification badges, access keys, and parking placards remain the property of MAA and must be surrendered upon demand.
17. I will return my MAA security identification badge to my company or MAA Badge Office immediately when it is no longer required for the performance of my duties, termination of employment or work assignment, or I am no longer associated with a hangar at MAA.
18. All lost, misplaced, or stolen MAA security identification badges or keys must be immediately reported to the signatory authority and thereafter to the Airport Security Coordinator (ASC) or their designee at MAPD in writing. The original, signed form must be received by the ASC no later than the next business day. Forms are available on the website at www.mlbair.com. There will be a $50 fee invoiced for the lost, misplaced or stolen badge.
19. If a badge holder has an expired, lost, misplaced, stolen, or forgotten their MAA security identification badge they are not allowed to be escorted or permitted within an area requiring a badge. Escorting a badge holder with an expired, lost, misplaced, stolen, or forgotten MAA security identification badge is a security violation.
20. Failure to return any MAA security identification badges or control access keys will subject you to a fine of $100 for each unreturned item and the additional cost incurred to re-core the lock and cut new keys. Upon signing the MAA security identification badge application, the badge applicant authorizes their signatory authority to invoice them or deduct from the applicant's wages the cost(s) associated for failure to return any MAA security identification badges or control access keys after they separate employment or affiliation with the airport.
21. Mutilation or alteration of any MAA security identification badges, access keys, and/or parking placards will invalidate these items. They are in no way transferable and may not be duplicated.

THIS APPLICATION MUST BE PRINTED IN COLOR

REV. SEP. 2021

22. If applicant/badge holder is required to operate ANY type of motorized vehicle on the ramp they must have ramp vehicle operations training. This training must be completed prior to the issuance of your initial badge and each time you renew your MAA security identification badge. You must present your valid Florida driver's license for verification. If you do not have a Florida driver's license you must provide verification from that state's Department of Motor Vehicles (DMV) that proves you possess a valid driver's license. You may not operate motorized vehicles or equipment in areas which you are not authorized for. (i.e. non-movement areas may not operate in any movement areas such as taxiways or runways.) Per FAA and MAA rules, regulations, and recommendations if a badge holder's driver license is suspended then their badge may be changed to reflect the removal of ramp driving authorization.
23. Renewal badge holders have 30 days from the date they renew their badge to attend a ramp vehicle operations retraining class. Again, you must present your valid Florida driver's license for verification. If you do not have a Florida driver's license you must provide verification from that state's DMV that proves you possess a valid driver's license.
24. MAA security identification badge holders operating motorized equipment on airport property or Ramp/AOA areas will ensure that all vehicle and passenger gates are locked or must be attended at all times. Personnel monitoring gates are responsible to ensure persons utilizing these gates are in compliance with MAA and TSA Regulations. Including verification of name(s) against the TSA Stop List. Gate monitors must keep a current Stop List in their possession at all times.
25. MAA security identification badge holders may ONLY escort a person in the AOA, SIDA, Secure, or Sterile area if they are a designated authorized escort. The MAA Security Identification Badge will reflect an approved escort with the green circled E insignia. If an applicant has been denied a badge they will be placed on a stop list and are NOT allowed to be escorted onto airport property where a MAA security identification badge is required.
26. Escorts must continually maintain visual and audible contact at all times with the persons under escort while within the AOA, secured area or SIDA in a manner sufficient to identify whether the escorted individual is engaged in activities other than those for which escorted access was granted. If a problem occurs, contact the MAPD for assistance.
27. After notification that an applicant's background has been completed, applicants must obtain their MAA security identification badge within 30 days of that notification. If the badge is not received within the 30 days, the CHRC must be processed again.
28. All MAA security identification badge holders must renew their issued MAA security identification badge before the expiration date which is listed on the front of the badge. You may renew up to 60 days prior to the expiration. Each time you renew your MAA security identification badge you must complete another MAA security identification badge application. Additionally, if you require Customs and Border Protection (CBP) area approval a separate application must be submitted to CBP and that approved application must be received in the MAA Badge Office prior to issuance of your renewal badge.
29. MAA security identification badge holders who do not renew expired badges within 30 days of expiration will need to complete a new MAA security identification badge application and undergo a new security threat assessment before a new MAA security identification badge will be issued. This process will take an additional business day to complete. An expired badge in excess of 30 days will require a longer vetting period. Use of an expired MAA security identification badge is a security violation and may result in denial of the MAA security identification badge renewal, criminal and/or civil penalties.
30. MAA security identification badge applicants and signatory authorities have a continuing obligation under 49 CFR 1542.209(l) to disclose to MAA within 24-hours if a MAA security identification badge holder is arrested or convicted of any disqualifying criminal offense that occurs while they have unescorted access authority.
31. If the CHRC or STA discloses information that would disqualify an individual from receiving or retaining unescorted access authority and the individual believes there may be an error in the CHRC, the individual must notify the ASC within 30 days of their intent to correct any information they believe to be inaccurate. It is the individual's responsibility to correct any areas they believe are not accurate in the CHRC.
32. MAA security identification badge holders or applicants may request a copy of their Federal Bureau of Investigation (FBI) CHRC by providing a written request to the Airport Security Coordinator.
33. MAA reserves the right to refuse or revoke authorization of any individual for MAA security identification badges where such action is determined to be in the best interest of airport security.
34. SCREENING NOTICE: Any employee holding a credential granting access to a Security Identification Display Area may be screened at any time while gaining access to, working in, or leaving a Security Identification Display Area.
35. No information may be released that may compromise the contents of MAA's Airport Security Program.
36. I fully acknowledge my security responsibilities as outlined in TSR 1540.105(a) – Security Responsibilities of Employees and other Persons, and will comply with all airport security rules. I further acknowledge that I may lose my access privileges or be subject to civil penalties for violating these rules. Authorized Signatories shall attest that an applicant acknowledges their security responsibilities.
37. I have read, acknowledge, and will comply with the MAA Rules and Regulations. Violations of any of the MAA Rules and Regulations and/or Applicable Code of Federal Regulations may subject you and/or your signatory authority to all penalties and fines that may be levied by MAA, TSA, or any other applicable government agencies, up to and including revocation of your MAA security identification badge.
38. No weapons permitted in the Airport Terminal (including Public and Sterile Areas), Security Identification Display Area (SIDA) or Air Operations Area (AOA) unless in accordance with local, state or Federal laws.
39. All Badging Rules and Regulations are under continuous review, and subject to revision. It is the responsibility of the badge holder to keep current with MAA badge holder Rules and Regulations. Rules and Regulations can be found on the MLBAIR.COM website.
40. MAA security identification badge holders who violate aviation security requirements resulting in an MAA security identification badge revocation, will have their information added to the CRD (TSA National Centralized Revocation Database) for a period of five (5) years.

THIS APPLICATION MUST BE PRINTED IN COLOR

APPLICANT MUST RETAIN THIS PRIVACY ACT NOTICE

The Privacy Act of 1974
5 U.S.C. 552a(e)(3)

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.

APPLICANT MUST RETAIN THE ESCORT AUTHORITY PROGRAM INSTRUCTIONS

Escort Authority Program

1. Employees authorized by their company to act as an escort for personnel who do not have unescorted privileges must be fluent in the English language.
2. The Escort Program applies to all areas within the perimeter of the Airport. (i.e. AOA, SIDA/Secured, and/or Sterile areas).
3. Must have an unexpired MAA Security Identification Badge with the green circled E insignia designating they are an authorized escort.
4. Escort only as many visitors as can be properly controlled; MAA recommends no more than 10 visitors per escort.
5. Accompany the visitor(s) at all times.
6. Must continually maintain visual and audible contact at all times with visitor(s) under escort.
7. Only allow the visitor(s) to go where the escort's badge has granted access.
8. Immediately notify the Melbourne International Airport Police Department (321-288-0147) when a visitor(s) engages in suspicious or in appropriate activities.
9. If a badge holder has an expired, lost, misplaced, stolen, or forgotten MAA security identification badge they are not allowed to be escorted or permitted within an area requiring a badge. Escorting a badge holder with an expired, lost, misplaced, stolen, or forgotten MAA security identification badge is a security violation.
10. If an applicant has been denied a badge they will be placed on a stop list and are NOT allowed to be escorted onto airport property where a security badge is required.
11. If you see an un-badged individual within the perimeter areas of the airport that is not under escort follow the proper challenge procedures.
12. *Challenge procedures are*:
    a. Approach the un-badged individual in a non-threatening and helpful manner and inquire as to the reasons why the un-badged individual is within the secure area portion of the Airport.
    b. When an un-badged individual cannot produce an MAA security identification badge, the individual conducting the challenge must escort the person out of the secure area and immediately report this incident to a Melbourne International Airport Police Officer for further investigation.
    c. If an authorized individual cannot approach an un-badged person for safety reasons, the authorized individual must keep close surveillance of the un-badged person and immediately contact a Melbourne International Airport Police Officer to report the incident.
    d. The 24 hour Melbourne International Airport Police Department (MAPD) emergency notification number is 321-288-0147, which is located on the back of the MAA security identification badge.
13. Escort privileges may be denied or revoked at any time.
14. I acknowledge and understand my responsibilities under 49 CFR 1540.105(a) as a MAA security badge holder who is being allowed escort authority privileges.
15. I am aware that any deviations to the aforementioned requirements may result in security violation and that I may be subjected to a TSA civil penalty pursuant to 49 CFR Part 1542 – Airport Security.

THIS APPLICATION MUST BE PRINTED IN COLOR

REQUIRED IDENTIFICATION TO ESTABLISH IDENTITY AND CITIZENSHIP STATUS - FROM USCIS Form I-9

ALL applicants must submit 1) proof of identity and 2) citizenship status and/or legal employment status. To meet those requirements the following is required; 1 document from list A is acceptable OR 1 document from list B AND 1 document from list C. All documents must be original and unexpired.

LIST A Documents that Establish Both Identity and Employment Authorization	LIST B Documents that Establish Identity	LIST C Documents that Establish Employment Authorization
1. US Passport or US 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. In the case of a nonimmigrant alien authorized to work for a specific employer incident to status, a foreign passport with Form I-94 or Form I-94A bearing the same name as the passport and containing an endorsement of the alien's nonimmigrant status, as long as the 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	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. US Military card or draft record 6. Military dependent's ID card 7. US Coast Guard Merchant Mariner card 8. Native American tribal document 9. Driver's license issued by a Canadian government authority For persons under age 18 who are unable to present a document listed above: 10. School record or report card 11. Clinic, doctor, or hospital record 12. Day-care or nursery school record	1. Social Security Account Number card other than one that specifies on the face that the issuance of the card does not authorize employment in the United States 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. US 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

THIS APPLICATION MUST BE PRINTED IN COLOR