



DETROIT METROPOLITAN AIRPORT

Wayne County Airport Authority

Security

Authorized Signer Handbook

BADGE ACCOUNTABILITY / BADGE RESPONSIBILITY

Airport Security Credentialing is an important factor in keeping the Airport safe and secure for all employees and the traveling public. A critical component in the Security Credentialing process is the designation of who is responsible for Airport Credential documentation, issuance authorization, record keeping, auditing, and most importantly, accountability. This handbook is designed for a company's Authorized Signer designee who is trained and authorized to approve badge issuance to new applicants and is the company representative responsible for the accountability of all Airport issued credentials.

As an Authorized Signer, you will need to be familiar with the credentialing process, identification requirements, access requests, security training, and above all, maintaining control and accountability for ID Badges issued to your company and making appropriate notifications to the Airport of any change in status. Please read this handbook carefully to familiarize yourself with the information. You can always contact the Airport's Credentials Office (734-942-3606) with any questions that you may have.

DEFINITIONS

Air Operations Area (AOA) – Defined as that portion of the Airport designed and used for landing, take-off, and surface maneuvering of airplanes.

Airport Security Program (ASP) – The guidelines established by the Airport that describe requirements for security programs and access control systems that are approved by the TSA.

Authorized Signer – An individual that has completed the necessary training and is authorized to approve credentialing forms to authorize issuance of Airport ID media.

Badge – A photo identification card that allows the individual to whom it was issued to access to security sensitive areas of the airport.

Badge Application – A form that must be completed before applying for an Airport ID Badge

CHRC – Criminal History Record Check is a FBI Fingerprint based background check.

Escort Authority – Special privilege that allows the holders of escort authority to provide escort to non-photo badged individuals while in the security sensitive areas. Icon is on ID Badge to identify this privilege.

Restricted Area - Any area of the Airport not open to the general public this includes employee parking areas.

Participant – Individuals who are employed at the Airport and are issued an Airport ID Badge.

STA – Security Threat Assessment (STA) that is completed by the TSA

Security Identification Display Area (SIDA) - The areas of the Airport that require ID Display at all times. Includes the Secured area and any area where cargo is stored, sorted, loaded or unloaded.

Security Sensitive Area – Includes the Sterile, Secured, SIDA and Air Operations Areas (AOA) of the Airport.

Sterile Area - Any public area located beyond a passenger-screening checkpoint

Secured Area - Any restricted ramp area adjacent to the terminal buildings. The Security Identification Display Area (SIDA) is within the Secured Area.

TSA – (Transportation Security Administration) Federal agency responsible for the screening of passengers and their property before departing on a flight and the oversight of the security at the Airport.

WARNING: Sensitive Security Information

Sensitive Security Information (SSI) is any information that is related to incidents that occur at the Airport and/or any information that could compromise security at the Airport.

As an authorized badge-holder, you may not discuss any security related incidents that occur at the Airport or provide details about the Airport's security system to anyone who does not have a need to know. If anyone tries to obtain information from you regarding the Airport's Security Rules and Procedures, report it to your supervisor, Airport Police or Airport Security immediately. Violation of the SSI regulation is a federal offense and punishable with a civil infraction and/or jail time.

AUTHORIZED SIGNER REQUIREMENTS

Each air carrier, tenant, vendor, government agency and contractor requiring access to the Security Sensitive Area must become a "Participant" in the Airport Security Program and must remain in good standing with the program to maintain Airport security badge issuance privileges.

Vendors and Contractors must be sponsored by the Airport, an airline or tenant. The sponsorship establishes that a vendor or contractor has legitimate business at the Airport. A company sponsoring a vendor or contractor must immediately notify the Credentials Office when any sponsorship is terminated. It is the Authorized Signer's responsibility to establish the sponsorships and to notify the Airport when a change has occurred or additional access is required for their contractor/vendor.

Each participant must designate an Authorized Signer(s) for their company to ensure their company's compliance with the Airport Security Program and act as a point of contact between the participant (company) and Airport Security. Each company's operation is unique so it is important to follow the guidelines below when designating an Authorized Signer(s). Authorized Signers:

- Must be an active Badge holder or applying for an Airport ID Badge.
- Must take and pass the Security Training Course.
- Must complete the Authorized Signer training annually.
- Must be in good standing with Airport Security by:
 - Never signing blank or incomplete forms
 - Preventing unauthorized access by reporting all lost, stolen, non-returned or terminated badges immediately
 - Establishing internal procedures for the notification and return of ID Badges that no longer require access at the Airport.
 - Acting as the primary contact for the Credentials Office
 - Read and distribute the Airport Security Newsletter (Good News/Badge News) to all employees
- Should assign more than one individual as an Authorized Signer so that employees are able to have their documentation authorized or access granted if an Authorized Signer is unavailable.
- Should be reasonable about the number of Authorized Signers for your company. There is a dedication of time to remain current as an Authorized Signer and a level of accountability for overseeing the ID issuance and tracking.
- Should work in the local area or at the Airport since they need to be available to their employees and to the Credentials Office.

Once a company identifies a person in a position of authority who will be the primary point of contact regarding Airport security badges, they will need to go through the Airport's computerized Authorized Signer training. This training will help them understand the credentialing process, documentation, identification and proper record keeping. The mandatory training is required annually upon badge renewal as long as they are an active Authorized Signer.

BADGE APPLICATIONS - RESPONSIBILITIES

Authorized Signers must ensure that each applicant has a reoccurring operational need to access the security sensitive areas of the Airport. They must review all completed applications to ensure they are complete, legible, and accurate before the application can be authorized (Use ink only - white out is not acceptable). The Authorized Signer must sign all pages and check for ramp, parking and escort access, if needed. Escort Authority must be justified and restricted to only those employees with an operational need. Stamped or photocopied signatures are not accepted. Applicants must submit the application to the Credentials Office within 30 days from the

Authorized signature date on the application. As an Authorized Signer your signature gives approval for badge issuance. Never sign a Badge application before the employee completely fills out the application. This is a violation and may lead to an Administrative Penalty and your Authorized Signer privileges may be revoked. **NEVER sign a blank application!** Your role as an Authorized signer

is to review and confirm all information listed on the application. You cannot perform these functions with an application that has not been completely filled out. Immediately report any lost application(s) to Airport Security.

- You must ensure that the applicant has the two forms of ID or documents that meet the federal requirements.
- You must visually verify the applicant's documents and check to make sure they are valid (must be originals and not expired). For applicants born outside the United States, additional citizenship documents are required. You must understand the requirements and be familiar with these acceptable documents (refer to the latest US I-9 form on the Department of Homeland Security – US Citizenship and Immigration Services).
- You must maintain a copy of the application and all forms in your file. This information is subject to audit by the Airport and the TSA.

BACKGROUND CHECKS AND BADGE ISSUANCE

Prior to Badge issuance, applicants must undergo a CHRC conducted by the FBI and a STA conducted by the TSA. The CHRC verifies that the individual has no convictions or current charges for any of the TSA disqualifying crimes within the past ten (10) years – go to www.MetroAirport.com under the badging toolbar for the full list of TSA disqualifying crimes. As an Authorized Signer, you are required to notify Airport Security within 24 hours if you, or one of your badged employees, have an arrest or conviction for one of the disqualifying crimes.

If the Airport disqualifies an individual from obtaining a badge due to the results of any of the background checks, an email or letter will be sent to the company and employee. The individual may be asked to provide additional documentation in order for the Airport to complete the background investigation.

Authorized Signers can check the status of an individual's badge approval as well as when their Badge was issued by going to the following link: www.apps.metroairport.com/badgesstatuscheck/ You must also make sure that the employee picks up their Badge within 30 days from the date of approval.

Any person who is disqualified from obtaining an Airport ID Badge may not be escorted into any security sensitive area of the Airport at any time for any reason. Anyone who knowingly authorizes or provides an escort for a disqualified individual will be subject to a security violation.

Badge applicants may be denied Badge issuance or the Airport may suspend the unescorted access privileges of current Badge holders due to an outstanding arrest warrant. The Airport conducts warrant checks on all individuals who are being issued, or are renewing, their Airport ID Badge.

All active badges are being continuously vetted for any new arrests or convictions of one of the TSA disqualifying crimes. Employees found to be newly charged with or convicted of one of these crimes will have their DTW ID Badges immediately revoked.

ACCOUNTABILITY

Badges that have been lost or stolen must be reported immediately to Airport Security. This notification will allow the Airport to “revoke” the lost or stolen Badge so that the Badge cannot be used to gain access. To replace a lost or stolen Badge, the individual must fill out a “Badge Replacement Form” and have it signed by the company’s Authorized Signer to verify the individual’s employment status.

It is the responsibility of each company to maintain accountability of all ID Badges issued to or pending issuance for their employees. Once an applicant reports to the Credentials Office for processing, it is your responsibility to notify the Airport if the applicant will not be issued a badge for any reason.

It is the responsibility of the Authorized Signer to maintain accountability of all ID Badges issued to their employees. Badges must be retrieved and returned to the Airport when an individual no longer requires access to any Security Sensitive Area, or if an employee resigns, is terminated, retires, laid-off, on strike, or is on medical or maternity leave. In these types of routine separations, Badges must be returned to the Credentials Office on a “Separation Form” without delay. If the Badge is not retrieved from the individual at the time of a routine separation, Security must be notified by telephone, fax, or in person, immediately in order to have the badge deactivated. Upon this notification, the Airport will “revoke” the individual’s access authority in the Security Card Access System, to prevent him/her from accessing any security sensitive area(s) of the Airport. A Separation Form must be completed and submitted, indicating the reason and date of separation and reasonable steps must be taken to retrieve the Badge. Once an employee submits an application to the Airport, you are responsible for notifying the Airport of separation, even if a badge has not yet been issued.

Failure to notify the Airport about any ID Badge that you can no longer account for is a violation of the Airport Security Program and will result in a ‘Failure To Notify’ fee of \$100.00. In addition, a \$100

‘Failure to Return’ fee will be assessed to your company if the ID Badge is not returned to the Credentials Office within (90) ninety days from the date of separation / deactivation. The ‘Failure to Return’ fee is non-refundable.

ESCORT AUTHORITY

The Airport is required to limit the number of individuals that can escort non-photo badged individuals in Security Sensitive Areas of the Airport. This is accomplished by the “Escort Authority” icon on the ID Badge. As an Authorized Signer, the request for an individual to have this special privilege must come from you. Please ensure that the individual’s need to provide escorts is valid before requesting the change from the Credentials Office.

BADGE RENEWAL

All badges expire at the end of the individual's birthday month. Failure to renew an ID Badge before it expires will result in the badging process starting from the beginning. A new application will be required and the individual will have to attend the Security Training in order to receive their ID Badge. In addition, a late renewal fee will be assessed to the individual and the company will be charged the new applicant fee.

As an Authorized Signer, it is part of your responsibility to make every effort to ensure that employees renew their badges on time.

AUDITS

The Airport Credentials Office will routinely audit your companies ID Badge records to ensure accuracy as required by Federal regulations. These audits include a listing of all active Airport ID Badges issued to your employees. You will be given a specific time period to review the list, ensuring that all individuals are still employed, still require airport access and are in possession of their Airport ID Badge. Upon return of a completed Audit, the Airport will review your audit to determine compliance and accountability. Random audits may be required where the company must supply the Airport with a list of active employees who have an Airport issued ID Badge.

In the event that Audit results are less than favorable, the Airport may require more frequent Audits or may require your company to undergo a Physical Audit. Physical Audits require each badged employee to report to the Credentials Office, within a specific time period, to have their Badge inspected and accounted for.

The Credentials Office may also audit your records. As an Authorized Signer you are required to maintain a copy of your employees Badge applications. These records must be maintained for the duration of time that the employee is with the company, and up to 180 days from the date of termination/separation and is subject to audit by the Airport and TSA.

Each company must provide the Airport with the location where employee badge records are stored and the name, title, and phone number of the individual who maintains the records. This information is retained by the Airport on the Authorized Signature or Delegation of Authority Form.

The Airport relies on you, as an Authorized Signer to assist us with enforcement and compliance with security rules and procedures associated with the issuance and accountability of Airport ID Badges. By knowing the Airport's security procedures, understanding your responsibilities and following important guidelines, you will have all the tools you need to be a successful Authorized Signer. Your support of the Airport's Credentialing system is expected and appreciated and helps to ensure a safe environment for everyone at the Airport.

The Airport will provide badge information and other related Security information to Authorized Signers electronically. In order for this to occur in an efficient manner, it is important that you update us with your contact information, including email address.

