DETROIT METRO • WILLOW RUN
WAYNE COUNTY AIRPORT AUTHORITY

AIRPORT SECURITY RULES & PROCEDURES

Call **855-MICHTIP**(855-642-4847)
or **9-1-1** in case of emergency.

If You See Something Say Something™ used with permission of the NY Metropolitan Transportation Authority.

June 2017

The Wayne County Airport Authority (WCAA) helps to safeguard the region's people and economy, so that residents and businesses alike can prosper with secure and efficient air travel. As a member of the airport community, you and your fellow employees play an important part in Detroit Metropolitan Wayne County (DTW) Airport's first line of defense against possible threats. You are responsible for ensuring that the Airport, its passengers, and your fellow employees and colleagues are both safe and secure.

This booklet contains security procedures and regulations derived from the Airport Ordinances and the Airport Security Program. The Airport Ordinances are available at www.metroairport.com. It is every employee's responsibility to be familiar with and to comply with the Airport's Security Rules & Procedures and for monitoring other individual's compliance with them. It is important that you take the time to review this important information.

Working together to serve the public at DTW, we depend on one another to be diligent in our jobs, aware of our environment and to report any suspicious persons, items or activity. Thank you for your support in our efforts to ensure safety and security at DTW.

INDEX

SECTION 1 – DEFINITIONS

Access Control System – Any portion of the Airport's electronic security system that provides/prevents access into Security Sensitive Areas of the Airport.

Airport Identification Badge – The identification required to access Security Sensitive Areas. Is issued to employees who are properly trained and approved by the Airport.

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

Challenge – The act of attempting to ascertain the authority or purpose of an unescorted person, not wearing or displaying Airport approved identification, to access or remain in the Air Operations Area, Security Identification Display Area (SIDA) or secure areas of the Airport, by directly requesting such person to display Airport-approved identification.

Disqualifying Offense – List of crimes that the TSA has identified where an individual that has been convicted or found not guilty by reason of insanity, in any jurisdiction, during the past 10 years, cannot be issued Airport approved identification. The Airport also maintains the right to deny badge issuance based on current criminal charges or other related activities that pose a threat to the Airport.

Escort - To accompany or maintain constant visual contact with ability to control actions of an individual who does not have unescorted access authority into or within a Security Sensitive Area of the Airport.

Piggybacking – Allowing the access of an unauthorized individual through a security door or gate during an authorized individual's entry into a Security Sensitive Area.

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

Secured Area - Any restricted ramp area adjacent to the terminal building. The Secured Area is also part of the Security Identification Display Area (SIDA).

Security Sensitive Area – Includes the AOA, Restricted, Sterile and Secured Areas of the Airport and requires all persons to possess a current, valid, Airport approved identification.

Security Identification Display Area (SIDA) – Includes the Secured and Cargo Areas of the Airport and requires all persons to possess a current, valid, Airport approved identification and to display their Badge at all times.

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

Tenant Leased Ramp – Ramp areas along the perimeter of the Airport that do not require temporary badge issuance for visitors but still require all visitors to be properly escorted by an Airport Photo ID Badged individual.

Visitor – Anyone that has not been issued an Airport Photo ID Badge and who requires access to a Security Sensitive Area.

SECTION 2 – 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 give out 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 is punishable with a civil infraction and/or jail time.

SECTION 3 – SECURITY ADVISORY

Depending on the current threat, the Airport and all Airport ID Badge holders may be subject to additional security measures and procedures. The Airport will advise you, through your employer, of any security requirements that directly affect you.

Please increase security awareness in your normal course of duties at the Airport by utilizing these guidelines:

- Support uniformed or plainclothes security or law enforcement officers by providing surveillance, acting as a deterrent and immediately reporting any suspicious activity or security-related incidents to Airport Police immediately.
- Be alert to any unattended baggage or suspicious activity or persons in parts of the Airport where passengers board or deplane, the ticket counters, baggage make-up areas, baggage claim areas, and the Airport perimeter. Report any suspicious activity or persons or unattended bags to Airport Police immediately.

SECTION 4 – SECURITY RULES & REGULATIONS

Each employee/Airport badge holder is required to comply with:

1. Federal, state and local laws and,
2. TSA regulations which include 49 CFR 1503 (Investigation and Enforcement), 49 CFR 1520 (Security Sensitive Information Protections), 49 CFR 1540 (Security Responsibilities of Employees) and 49 CFR 1542 (Airport Security Rules) and,
3. WCAA Security Rules and Procedures which are based on the Airport Security Program (ASP) and the Airport Ordinances.

Rules covered in this booklet are taken from the above mentioned sources. Violation of the rules, regulations, laws and procedures may be cause for a security violation to be issued.

All persons and their property are subject to inspection while on Airport property.

The Airport will suspend the unescorted access privileges of anyone with an outstanding arrest warrant.

As an employee, you MUST notify Airport Security if you have been charged with, or convicted of, a Felony or a weapons offense.

SECTION 5 – ID BADGE ACCESS AREAS/COLORS

A person shall not enter any Security Sensitive Area unless the Airport has first issued a valid Airport ID Badge authorizing his/her access. An Airport ID Badge does not authorize access to the entire Airport.

Airport ID Badges are issued to support your job duties and responsibilities at the Airport and should be used for official business purposes.

A person may not tamper, damage, interfere with, compromise, modify, attempt to circumvent, or cause a person to tamper, damage, or interfere with, compromise, modify, attempt to circumvent any security system, measure, or procedure.

Badge holders are only authorized to be in the area denoted by the color of their Badge. The following Badge colors and access areas are currently in use at the Airport.

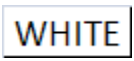
Access to Airline ramp areas and associated facilities and sterile area access. Red badges will be assigned to Airline personnel. Red badges with a Yellow Secondary color are assigned to Governmental agencies.

Access to tenant facilities. Blue badges with Red Secondary are assigned to tenants requiring AOA/Secured area access to the main ramp area.

Brown badges are assigned to corporate and perimeter tenants and allows access at their facilities. If access is required in an airline area, the badge will have a Red secondary color.

Access for vendors and visitors, as required.

Access to approved construction sites only.



"MUST BE SCREENED" General Identification Badge. Individuals must be screened prior to entering the sterile or AOA areas. White Badges are valid for unescorted access to the sterile area and escorted access in the secured area only after submitting to the TSA screening process at one of the passenger screening checkpoints. These badges are issued to vendor and concessionaire employees who work in a sterile area or restricted area. These employees cannot utilize any of the employee screening locations to gain access to the sterile or restricted areas.

Non Airport ID badged Airline Flight Crew employees, while in uniform, are allowed access through certain security doors that lead into their airline operational areas. DTW Badged employees that can verify the airline personnel can allow the uniformed flight crew access through security doors so that they may gain access to operations areas. Uniformed Airline Badged Flight Crew are allowed on the AOA in the footprint of the aircraft that they are assigned and to and from their operations area. Airline Flight Crew employees who have been issued an Airport ID Badge must utilize that badge for access through security doors and cannot gain access by other means.

SECTION 6 – LOST OR STOLEN ID BADGES & ACCESS MEDIA

Lost or stolen Airport ID Badges, keys, parking passes or other access media must be reported immediately to Airport Security. Security will deactivate the ID Badge so that it cannot be used for access. If you find your ID Badge, contact Airport Security to have the ID Badge reactivated in the security system. Do not attempt to use the ID Badge until you have been directed to do so by Airport Security.

Replacement Badge Fees:

- 1st replacement - $100 ($20 processing fee, $80 deposit)
- 2nd replacement - $200 ($20 processing fee, $180 deposit)
- 3rd replacement* - $300 ($20 processing fee, $280 deposit)
  *At the discretion of the Airport Security Chief

All lost Airport ID Badges, when found, must be returned to the Airport Security Credentials Office; replacement deposits will be refunded at that time.

SECTION 7 – ID BADGE RENEWAL

Airport ID Badges expire at the end of the month on the date indicated on the Badge (In most cases coincides with the badge holder's birth month). All Badge holders are responsible to report to the Credentials Office prior to this expiration date to have their Airport ID Badge renewed. Badge holders may renew their badge one month prior to and during the month of their birthday.

For renewal, two (2) pieces of valid identification are required. At least one ID must have been issued by a Government authority and at least one must include a photo. Applicants must provide documentation that establishes both their identity as well as their employment eligibility. For a list of acceptable documents visit the badging link on the Airport's website (www.metroairport.com). Employees may be required to undergo an FBI Fingerprint-based records check every two (2) years upon their badge renewal.

Badges that are not renewed by the end of the expiration month will be deactivated in the Electronic Security System. Expired

Badges are no longer valid and may not be used for access or identification. Do not attempt to use an expired Badge and do not allow another employee with an expired Badge to access any Security Sensitive Area. Failure to renew your Badge prior to the expiration will result in the requirement to re-apply for issuance of an ID Badge. This will require a new Badge application and FBI Fingerprint-based records check. You will not be issued an ID Badge until the Airport has reviewed the results and can confirm that you are eligible for Badge issuance. Late renewals result in a retraining requirement and the assessment of a "Late" fee.

If you have Customs clearance, 1st report to the Customs and Border Protections (CBP) office to renew your Custom seal and be approved prior to reporting to the Credentials Office. Failure to renew your Custom seal prior to reporting to the Credentials Office will result in the removal of your seal from your ID Badge.

SECTION 8 – BADGE RETURN

All Airport ID Badges and keys are the property of the Airport. You must return your Badge and keys when you no longer require reoccurring access at the Airport. This includes: resignation, transfer, retirement, lay-off, medical leave, termination, leave of absence, or when the construction project you are working on has been completed. The ID Badge cannot be kept for warranty work after a construction project. You must notify the Airport immediately when you no longer require access at the Airport.

Failure to notify or return your Airport ID Badge is a violation of the Airport Security Rules & Procedures and may result in the assessment of a "Failure to Notify or Failure to Return" fee.

SECTION 9 – VISITORS/ESCORTING

Only individuals who possess a valid Airport Photo ID Badge, and who have "escort authority" clearly identified on their badge, may escort visitors who possess a valid non-photo Airport ID and who have an operational need to be in a Security Sensitive Area. You cannot escort anyone who possesses and displays an Airport Photo

ID Badge. Each individual must utilize their own ID Badge to gain access into Security Sensitive Areas.

You may not escort any individual that has been denied an Airport ID Badge by the Airport (see #2 below for name check requirement).

To escort means to accompany or supervise an individual who does not have unescorted access authority to a Security Sensitive Area. Escorting rules require that you:

1. Ensure that the person being escorted possesses a valid non-photo Airport ID Badge (regardless of age) and has it displayed while in a Security Sensitive Area.
2. Contact Airport Security to conduct a name check of any individual you intend to escort.
3. Remain under visual and verbal control of the individual at all times while in a Security Sensitive Area.
4. Escort the individual both onto and out of the Security Sensitive Area.
5. Individuals possessing a White Badge may be escorted into the secured area after they have submitted to the TSA screening process and they are accompanied by an individual with a valid Airport Photo ID Badge with escort authority.

Visitors to perimeter tenant leased areas are not required to be badged; however they must comply with the existing Airport procedure for physical or visual escort by an authorized person who possesses a valid Airport Photo ID Badge. Tenant leased areas are located at buildings that form part of the Airport's perimeter.

SECTION 11 – EMPLOYEE PARKING LOTS

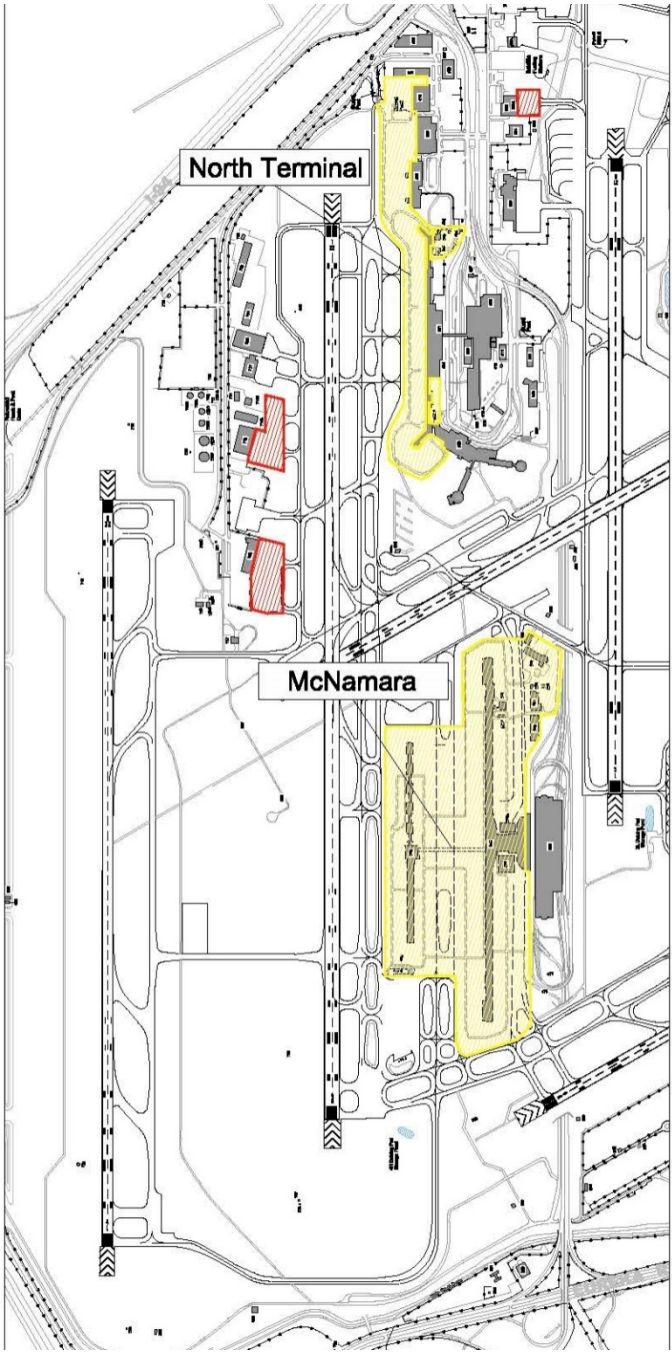
Authority to access employee parking lots must be authorized by your company and designated areas are assigned based on operational need. Access is granted through your Airport ID Badge and you are only required to swipe your Airport ID Badge (no PIN is required) to gain access. Do not allow anyone access into the restricted parking areas whose Airport ID Badge does not allow them access. Contact Airport Security immediately if you experience any problems accessing a restricted parking area or to report any damage to any parking/security equipment.

SECTION 12 – SECURITY IDENTIFICATION DISPLAY AREA (SIDA)

Transportation Security Administration (TSA) regulations (CFR 49, Part 1542.205) require individuals to continuously display their Airport Identification Badge while in the SIDA (Security Identification Display Area). The ID Badge must be visible above the waist (with photo showing) on the outermost garment.
The Airport's SIDA is defined as the Secured and Cargo Areas. Activities or entities on or adjacent to the SIDA include the following:

- The ramps of Buildings #514, #516 and #518 (Delta buildings).
- The North Terminal ramp area bounded by the taxiway Kilo from the approach end of 22L to K-5.
- The McNamara Terminal Ramp area bounded by the intersections of taxiways Uniform, Kilo, and Juliet from J-7 to Fox.
- Airline baggage make-up rooms / transfer areas.
- Airline loading ramps and aircraft facilities.
- Adjacent tenant and concession facilities.
- Wherever cargo is stored, sorted or loaded and unloaded onto an aircraft. This includes perimeter buildings such as Buildings #427-UPS, #530-Signature, #536-Delta, #614-Common Use #714 – DHL including the wide body apron, and #723 - FedEx.

In general terms, if you are exiting a security door from any concourse or gate area that leads to the Secured Area or a baggage make-up area, this is considered the SIDA and your ID Badge should be displayed as described above. SIDA may include operational areas and hallways inside the building. Failure to properly display identification while in the SIDA is a violation of the Airport Security Program, and could result in an Administrative Penalty issued by the Airport as well as a TSA violation and civil penalty. N**ote:** The SIDA boundary may change due to increased security levels. Should this occur, signage will be posted in affected areas.



Cargo Areas Secured Areas

SECTION 10 – CHALLENGING

"Challenging" is an inquiry as to whether an individual is authorized to be in a Security Sensitive Area. All Airport employees are required to challenge those individuals not displaying an Airport ID Badge while in a Security Sensitive Area or whose badge does not have the proper access color. This includes your co-workers and employees in uniform where their ID Badge is not visibly displayed.

Failure to properly challenge is a violation and may result in an administrative penalty.

Procedure for Challenging:

1. Approach the individual and request to see his/her Airport ID Badge. If the individual is unable or unwilling to produce a valid Airport ID Badge (with the correct access color), escort him/her from the Security Sensitive Area staying with the individual and immediately report the incident to the Airport Police or Airport Security. Do not just let the individual go.
2. Should the individual refuse to be escorted out of the Security Sensitive Area, do not, under any circumstances, attempt to apprehend or detain him/her. Immediately report the incident to the Airport Police and monitor the individual's whereabouts.

SECTION 13 – VEHICLE ACCESS PROCEDURE

A vehicle may not be driven onto or within the AOA or Secured Area unless:

1. The driver of a vehicle has a valid Airport Photo ID Badge with the Ramp Access designation and;
2. The vehicle displays a valid DTW vehicle permit and;
3. The driver has taken and passed the "Ramp Driving" portion of the Airport Security Training.
    - Some employees may be required to undergo Ramp Safety training with Airfield Operations, prior to authorization.

When accessing manned vehicle checkpoints, wait until the vehicle in front of you has cleared before proceeding. To prevent unauthorized access, monitor the gate closely and wait until the gate is fully closed before leaving the area. Ensure that all passenger's badges have been provided to the Security Officer for verification.

Ensure that you follow the direction of Security personnel at all times. Remember to inspect your vehicle for hidden items or unauthorized personnel prior to gaining access to the AOA. It is the driver's responsibility to notify the security officer of any passengers contained in the vehicle for identification verification. All vehicles accessing the AOA are subject to vehicle inspections.

To prevent damage to the automatic gates and your vehicle, wait for the gates to fully open before proceeding through. Security enhancements, such as reinforced gate arms, are located at vehicle checkpoints so employees are advised to drive slowly and cautiously when driving through an automatic gate.

In order to access the Secured Area (see map), you must either access through a manned security gate or ensure that all vehicle

occupants have swiped their badge in a card reader and received authorization by the security card access system.

For safety reasons, pedestrian access is not permitted through any vehicle checkpoint. In addition, no motorcycles or bicycles are allowed on the AOA.

SECTION 14 – ELECTRONIC SECURITY SYSTEMS (ESS)

The Airport is secured by several different types of security systems. Some of the systems include; card readers, perimeter detection, Intellikey, CCTV just to name a few. Card readers are installed on doors and gates that lead to Security Sensitive Areas.

Each person accessing a door controlled by this system must individually swipe at the card reader and be authorized before proceeding through. Unless under direct and continuous escort (with proper visitor credentials, escort authority and name check), you are not to allow other badge holders to **piggyback** (allow someone access through a door on your card swipe). Should you or a coworker experience access problems, under no circumstances are you to access or allow them access through the door. Should you experience a problem gaining access, contact the Airport Response Center.

High winds or unknown maintenance issues may prevent doors and gates from closing properly. Employees are responsible for making sure doors and gates are properly secured before leaving the area to prevent unauthorized access. **Physically close doors by pushing or pulling the door to ensure that it is secured.** Report any maintenance issues to the Airport Response Center immediately.

Not all, but many security doors have local alarms. It is the responsibility of all Airport ID Badge holders to react to these alarms; secure the area, identify the problem and contact the Airport Response Center.

If you accidentally activate an alarm at a door secure the door immediately. Stand by the door until an Airport representative arrives and/or call Airport Response Center. When the Airport representative arrives, explain how the alarm was activated and provide any information requested.

Tampering with (i.e. preventing a device from working the way it was intended), or in any way compromising the security systems, will result in an administrative penalty or forfeiture of Airport ID Badge privileges and/or criminal prosecution. Do not alter or copy your ID Badge or post it on social media.

Should you cause (or observe) damage/tampering to any door, gate, fence, camera, or any security device, report it immediately to the Airport Response Center. If the damage results in an unsecured opening remain in the area to control unauthorized access until an Airport Representative arrives.

SECTION 15 – BOARDING DOORS

Some doors have the ability to be set into **hold-open mode** for the purpose of boarding or deplaning an aircraft. This function is an "attended function" and the door should never be left unmanned while in this mode.

While the door is set in the "hold-open" mode, employees working the flight (going only to the aircraft and not onto the AOA) need only swipe their Airport Photo ID Badge for authorization the first time through the door. The individual who sets the door in hold-open mode is responsible for ensuring that only authorized individuals are able to gain access. Subsequent access through the boarding door, for access to the aircraft, does not require an additional card swipe.

When boarding or deplaning an aircraft, you are required to closely monitor the door to ensure only valid passengers and authorized

personnel are allowed access. Once boarding or deplaning is complete, immediately secure the door.

If the door is in "hold open" mode and an individual requires access to the ramp, AOA and/or Federal Inspection Area (FIS), they are required to swipe and receive authorized access at the reader every time they access the door. The gate agent is required to verify access via the card reader prior to allowing access through the open door. If an individual receives a lockout at the boarding door, the gate agent should deny them access.

Flight Crews that have Airport ID Badges must use their badge to gain access through the boarding door. If for some reason an individual's badge does not work in the card reader, you should not let the individual through the door and contact the Airport Response Center to advise them of the situation.

Remember, regardless if a door is in hold-open mode, Airport Badged employees are required to swipe at the card reader and be individually authorized through the card access system.

EXCEPTIONS:

- Federal deportation agents that are required to visually observe the departure of deportees on an aircraft are authorized to remain on the jet bridge, without an Airport ID Badge, until the plane departs.

SECTION 16 – BAG-BELTS

You must use the card reader to open bag-belt doors and activate the belt controls. Once your Airport ID Badge has been accepted by the security system you may operate the belt system. Ensure that the auxiliary green light is on, indicating that the bag-belt door is completely down and secure, before leaving the area. The red light will remain on while the bag-belt door is open to indicate that the door is open/unsecured.

Once you open the bag belt doors and until the doors are closed or someone else takes over for you, it is your responsibility to observe the area and keep it secure by ensuring no unauthorized persons or bags are introduced into the system. Whenever another person takes control of the area, he or she need to swipe their Airport ID Badge in the card reader. This does not require that the system be stopped and the door to be shut. Have the individual simply swipe their Airport ID Badge in the card reader prior to you leaving the area. The last individual swiping in the card reader has responsibility for the bag-belt. If you leave the area and the bag-belt door(s) are not yet secured properly, you could be subject to an Administrative Penalty.

SECTION 17 – MICROWAVE GATES

Microwave gates are located around the Airport perimeter at Delta's Cargo Building #536 and Endeavor Airlines Maintenance Building #359. These gates allow for access from the tenant leased ramp areas onto the Airfield. Because these areas provide airplane access, microwave gates are used instead of physical gates or barriers.

The microwave gates require the use of the card readers before leaving the tenant ramp space and entering out to the Airfield. Everyone in the vehicle (unless under escort) must swipe their Airport Photo ID Badge in the card reader before accessing the Airfield. The vehicle's driver is ultimately responsible for ensuring only authorized individuals gain access to the Airfield, so the driver should observe the card swipe(s) and hear the audible alert to confirm the passenger's eligibility for access. If an individual does not receive a valid card read, the individual should not be allowed access to the Airfield. Failure to swipe before entering the Airfield is a security violation and may result in an Administrative Penalty. These gates are denoted with pavement markings and signage. For safety and security reasons, pedestrian access through microwave gates is strictly prohibited; only vehicle access is allowed.

SECTION 18 – SECURITY SCREENING

All individuals who are flying out as passengers on a flight must submit to TSA passenger screening – there are NO exceptions. When flying out, you may enter the sterile area only after your person and property have been screened by the TSA **(use of the AOA shuttle bus or security doors is not permitted**). Once you have submitted to TSA passenger screening you must remain in the Sterile Area. If you leave the Sterile Area for any reason, you must resubmit to the screening process. It is strictly prohibited to use your ID Badge to allow yourself or other personnel departing on a flight access to a sterile area without them or their belongings being properly screened at a passenger screening checkpoint. When flying out, you are not allowed to leave the Sterile Area without being rescreened by the TSA – this includes accessing the Secured Area.

Employees entering the secured or sterile areas from the public area will be subject to employee screening and all bags will be inspected to ensure that there are no weapons or prohibited items. Employees will be screened at the TSA screening checkpoints, employee parking lots or at terminal doors prior to entry into the restricted area.

Failure to comply with the screening requirements could result in an Administrative Penalty.

SECTION 19 – PROHIBITED ITEMS

The carrying of prohibited items in the Sterile or Restricted areas of the Airport is strictly prohibited. Prohibited items include weapons, explosives, incendiaries, and other items that are seemingly harmless but may be used as a weapon. A full list of all the prohibited items can be viewed on the TSA's website www.tsa.gov. Civil and/or criminal penalties may apply to any individual in possession of prohibited items in a Security Sensitive Area without prior authorization or approval.

Employees with an essential need for tools in order to complete their job duties are allowed those tools. The employee is responsible to ensure the tools are accounted for at all times and never left unattended in the Sterile Area or accessible to passengers.

The Airport Ordinances prohibits the carrying of a concealed pistol by a person with a valid concealed pistol license (CPL) issued by the State or any other State when the TSA or employee screening process has begun or when entering into, or while in, any of the Security Sensitive Areas of the Airport. Leave it at home!

SECTION 20 – ADMINISTRATIVE PENALTY

The Airport reserves the right to impose an administrative penalty and suspend or terminate the unescorted access privileges of any Airport ID Badged employee. Administrative penalties and/or badge suspension/termination shall be the direct result of an attempt to bypass the Airport badging system, compromise Airport security, violate the Airport's Security Rules & Procedures or the Airport's Security Program. Duplication, tampering or destruction of any badge, pass or device that allows access into a restricted area is strictly prohibited and punishable by suspension and/or civil penalty. Failure to secure doors or gates, conduct a proper challenge, prevent piggybacking, and properly display Airport ID Badges while in the SIDA are also grounds for administrative action.

Administrative Penalties are:

- 1st offense - $100.00
- 2nd offense - $250.00
- 3rd offense - $500.00
- 4th or subsequent offenses - $1,000.00 and a 30-day suspension, or permanent revocation.

As an incident occurs, Security will issue a Security Incident Investigation Notice (SIIN) to the possible violators. The SIIN advises the company and violator(s), that Security is investigating a possible security incident. This is the time for the violator and

his/her supervisor to submit a statement regarding the incident. Security will review the violator's statement and all reports regarding the incident to determine if there are extenuating circumstances that should be considered. The company and employee will be notified once a decision has been rendered.

Security violations that are more serious or flagrant in nature may result in up to a 30 (thirty) day Airport ID Badge suspension or a permanent revocation of unescorted access authority. When the Airport imposes an administrative penalty, the individual has 10 (ten) days to undergo retraining and either pay or appeal the administrative penalty. An employee may appeal an administrative penalty/suspension/termination by completing an "Appeal Form" which may be obtained from Airport Security. There is a non-refundable $25.00 administrative fee for the appeal process which must be submitted at the time of the appeal.

TSA Civil Penalty action initiated against the Airport as a result of a security violation will be passed on to the employee and/or the employee's Company.

Any individual found responsible for a piggyback violation will lose access privileges at that access point for ninety (90) days.

Any individual found responsible for an escort violation will lose their escort authority privileges for ninety (90) days.

SECTION 21 – REMINDERS

- **DO** wear your Airport ID Badge on your outermost garment above your waist (with photo showing) while in a Security Sensitive Area.
- **DO** challenge unbadged individuals or those who do not have the proper badge color while in a Security Sensitive Area.
- **DO** stop and display your Identification Badge when challenged, and to security officers at the manned vehicle checkpoints.
- **DO** ensure that no unauthorized person or objects are contained in your vehicle when accessing the AOA.
- **DO** ensure that all Airport Badged individuals accessing a jetway door that is open for boarding utilize the card reader for

access and received approval prior to allowing them through the open door.

- **DO** securely close any security door/gate opened by you, being sure that no unauthorized person(s) enters while the door/gate is open.
- **DO** immediately report lost or stolen Airport ID Badges or keys to Airport Security.
- **DO** keep your badge in good working condition. If your badge becomes damaged, through normal wear and tear, report to the Credentials Office to have it replaced at no charge.
- **DO** immediately return your Badge to your employer or Airport Security upon termination, resignation, transfer, leave of absence, medical leave, lay-off, retirement, or if you no longer require access at the Airport.
- **DO** notify Airport Security of any change in your name, address, email or phone number(s). Failure to respond to a request or notification from Airport Security may result in permanent revocation of access privileges.
- **DO** notify Airport Security within 24 hours of being charged with any disqualifying criminal offense.
- **DO** report any suspicious activity or unattended items to Airport Police or Security immediately.
- **Do** use your badge to access Security Sensitive Areas for official related activities.
- **NEVER** possess a dangerous weapon in any area of the Airport.
- **NEVER** fail to comply with the direction of individuals conducting employee screening, i.e., TSA or contract security.
- **NEVER** lend your Airport ID Badge or keys to anyone.
- **NEVER** tell anyone what your PIN is for your Airport ID Badge.

- **NEVER** escort anyone without first having a name check conducted by Airport Security.
- **NEVER, under any circumstances**, allow piggybacking through the card access system unless escorting an individual with a valid Non-Photo ID Badge.
- **NEVER** assume that someone looks like they belong, always challenge anyone if you do not see an Airport ID Badge.
- **NEVER** prop open any security door/gate or otherwise interfere with any lock or closing mechanism.
- **NEVER** walk through a vehicle checkpoint or microwave gate.
- **NEVER** allow any individual departing on a flight access to the Sterile Area without submitting to the TSA screening process.
- **NEVER** take luggage or other articles for a passenger departing on a flight into the Sterile Area without first submitting to the TSA screening process.
- **NEVER** leave any tool(s) or other prohibited items unsecured or unattended in the public areas of the terminals.
- **NEVER** allow access to the Security Sensitive Area to any individual who is experiencing access issues with their Airport ID Badge.
- **NEVER** copy, duplicate or alter your Airport ID Badge or other Airport access media or post it on social media.

IMPORTANT PHONE NUMBERS

EMERGENCY	**911**
Airport Security	(734) 942-3606
Airport Response Center	(734) 942-5304
Police/Fire/Security 24 hour dispatch	
Airfield Operations	(734) 942-3685

Airport Security
31399 East Service Drive
Building 610
Detroit, MI 48242

E-mail Security at:
security@wcaa.us

You may access Credentials Office related information and forms on the Airport's website www.metroairport.com just click on "Badging" on the toolbar.

DETROIT METRO • WILLOW RUN
WAYNE COUNTY AIRPORT AUTHORITY

6/17