



# Security Standards

Charlotte Douglas International Airport (CLT)
P. O. Box 19066
Charlotte, NC 28219

Telephone: 704-359-4000

www.cltairport.com

35 12' 53" North, 80 56' 18" West

749' MSL

# I. Revision Checklist

| | |
|---|---|
| All paragraphs are numbered for ease of search<br><br>**Added:** Section for visitors, section for construction AS<br><br>**Updates:** Definitions, Inappropriate Conduct Section, Chapter 9, Attachment 3 | May 2021 |
| **Added:** notice about deliveries into the Sterile Area<br>**Updates:** Definitions, Badge colors, Language for Bypassing security measures, Visitor Pass requirements, CLT Security Computer Systems, clarifications in the section 7.7 – Escorting, | June 2022 |
| **Added:** Definition for "Event", Section 6.4 - Concessionaires, Section 7.4.1 – Securing belt access,<br><br>**Updates:** Section 7.3.1 – Prohibited Items, Section 7.6 – Reporting Suspicious Activity, Section 8.1 – Clear Bag Policy, Section 8.4 – CCTV System | May 2023 |
| **Added:** Notice about employee screening, Section 4.2.1 and Appendix 3. Section 5.4.1 Requirement for submitting accurate biographical information.<br><br>**Updates:** Definition for Dangerous Weapon, Renaming of Citation to Notice of Violation throughout the document, | August 2023 |
| **Added:** A stipulation that anyone carrying out a security function must be badged (Section 6), Prohibition to use a key to bypass a card reader (Section 7.2), record video and audio (section 7.6), tailgating (Section 8.2.1), and piggybacking (Section 7.4). Requirement to wait at gates for an inspection (Section 8.2.1).<br><br>**Updates:** Title of Section 7.6. Clarifications for violations alignment and badge suspensions in Section 9. | May 2024 |
| **Added:** Definition and conditions for Local Interim Disqualifier (Section 5.6.1)<br><br>**Updates:** All workers entering the Sterile Area under a visitor pass must be escorted (Section 4.1.2), Clarification on video and audio release (Section 7.6), Escorting clarification (Section 7.7 b) Updates to Tier 3 and Tier 1 and 2 Violations table (Section 9), Removal of Clear Bag requirement (Section 8.1), Rearranged section 7.4 and 9 for better readability. | January 2026 |

## Contents

| **II. Appendices** | |
|---|---|
| Appendix 1 | Security Areas |
| Appendix 2 | Disqualifying Crimes |
| Appendix 3 | Security Identification Badge Rules and Regulations |

# 1 Purpose and Background

Welcome to Charlotte Douglas International Airport. Every Airport User, their employees, and subcontractors play a vital role in ensuring CLT provides and maintains a safe and secure environment. The Transportation Security Administration ("TSA") is the federal agency with responsibility for establishing and enforcing security regulations and for conducting passenger screening operations that are consistent with policies and directions from Congress. In collaboration with the TSA, CLT also has several areas of responsibility for security, including creating and enforcing airport security procedures, providing security training, establishing an airport Badge system, controlling and monitoring access to all areas of the Airport, and providing law enforcement and emergency response support.

In order to work or conduct business at CLT, most individuals will be required to obtain an airport Badge, display it at all times while at CLT, and adhere to the contents of these CLT Security Standards ("Security Standards"), the Airport Security Program ("ASP") and all applicable laws, regulations, directives, and policies while *anywhere on Airport property*. Further, no one shall tamper with or interfere with, compromise, modify, or attempt to circumvent any security system, measure, or procedure implemented pursuant to the ASP or cause another person to do so.

When necessary, major updates to Security Standards will be issued by CLT via Aviation Director's Notices, Operational Impact Notices, or other communications channels. Employers are responsible for ensuring that their employees read and understand the Security Standards and each update thereafter to ensure they have the latest information necessary to support the CLT security program and avoid unfortunate and preventable violations. The Airport Security Coordinator ("ASC"), where allowed by the ASP or federal regulations, may make exceptions in his or her sole discretion where such is in the best interest of the Airport.

# 2 Definitions and Abbreviations

**Access Media –** CLT-issued identification media/access credential ("Badge"), or access key ("Key") and encoded security key ("Security Key") that allow access into restricted areas.

**Air Operations Area (AOA) -** A portion of an airport specified in the Airport Security Program, in which security measures specified in 49 CFR Part 1500 are carried out. This area includes aircraft movement areas, aircraft parking areas, loading ramps, and safety areas for use by aircraft regulated under 49 CFR Parts 1544 or 1546, and any adjacent areas (such as general aviation areas) that are not separated by adequate security systems, measures, or procedures. This area does not include the Secured Area.

**Aircraft Operator 1544** – The operation of aircraft by operators holding a certificate under 14 CFR part 119 whose employee Badge applications will be processed by CLT after receipt of a complete and accurate application that includes the most recent Offense Cycle Number (OCN) and date from the designated Authorized Signer.

**Airport Operator 1542 -** The operation of airports regularly servicing aircraft operations and who conduct fingerprinting and adjudication for its employees, subcontractors, and vendors, Airport Tenants and their subcontractors, Foreign Aircraft Operators 1546 and their subcontractors and subsidiaries, and the subcontractors of Aircraft Operators 1544.

**Airport Security Program (ASP) –** A security program approved by TSA under § 1542.101 of 49 CFR Chapter XII.

**Airport Tenant –** Any person, other than an Aircraft Operator or Foreign Air Carrier, that has a security program under Parts 1544 or 1546 of 49 CFR Chapter XII and a lease agreement with the Airport to conduct business on airport property, with the exception of Concessionaires and construction contractors.

**Airport Security Coordinator (ASC) -** Primary contact for security-related activities and communications with the TSA and Airport Tenants.

**Airport User** - Means Airport Tenant, Air Carrier, Concessionaire, Contractor, or Vendor collectively.

**Authorized Signer (AS) –** Any individual or designated representative authorized to sponsor individuals, collect and transmit biographical data to the Credentialing Office, and request airport Access Media.

**AS Web Portal** – A website that allows AS secure access to manage the Badge holders for the Airport User.

**CCTV –** Closed Circuit Television, a system for video surveillance at CLT.

**Centralized Revocation Database (CRD) –** Centralized database of individuals whose Badges were permanently revoked for failure to comply with aviation security requirements. The database is maintained by the DHS.

**Charlotte Douglas International Airport (CLT or Airport)** – Terminal and all other associated properties that are covered by the TSA-approved Airport Security Program, including, without limitation, parking facilities, cargo warehouses and operations, and the Fixed Based Operator and associated general aviation activities.

**CMPD –** Charlotte Mecklenburg Police Department; primary Law Enforcement Officer (LEO) response at CLT.

**CHRC** – Criminal History Records Check; fingerprint-based background check.

**Concessionaire** – An employee of any entity that has an agreement with the Airport Operator to conduct business in the Sterile Area. Sterile Area Concessionaire Employees include employees of restaurants, specialty stores, kiosks, and non-airline sponsored lounges and clubs located in airport Sterile Areas. The term "Sterile Area Concessionaire Employee" does not include an employee of airport operator, aircraft operator, or foreign air carrier that has a security program under 49 CFR Parts 1542, 1544, 1546; this term also does not include Federal, State, or local government officials.

**Contractor –** An entity whose function is project or maintenance-related. It includes, without limitation, design firms, construction consultants, management companies, and facilities maintenance providers. Companies involved in construction activities are considered contractors regardless of their leasing space at the Airport.

**Credentialing Office –** Office where Airport Users obtain background checks, Badges, and required regulatory training. It is located in baggage claim, near the international arrivals. Information on hours of operation can be found on the website www.cltairport.com/business/credentialing.

**Dangerous Weapon -** Certain objects or devices designed or intended to be used to inflict serious injury upon persons or property, including, but not limited to, firearms (loaded and unloaded), including ammunition;; all switchblade, double bladed, or butterfly knives regardless of length, razors and razor blades, except when used solely for personal shaving; dynamite cartridges, bombs, grenades, mines, and other powerful explosives; slingshots; shurikensand similar items; self-defense spray.

**Disqualifying Crime –** An applicant has a disqualifying criminal offense if that person has been convicted of, or has been found not guilty by reason of insanity, of any crime listed in TSR 1542.209, or 1544.229. (See Appendix 2).

**DR (designation on Badge) –** Designates persons authorized to drive on the AOA unescorted

DR-E (designation on Badge) – Designates persons authorized to perform vehicular escorts in the non-movement area specifically for personnel with an official business need to access the AOA who lack the DR endorsement.

**Escort –** Means to accompany or maintain constant visual contact with an individual who does not have unescorted access authority into or within a Secured Area or SIDA.

**Personnel ESCORT (yellow "ESCORT" designation on Badge) –** Individuals authorized to accompany or escort unbadged individuals in the restricted areas. This does not include the authority to perform vehicular escorts.

**Event –** is defined by one or a combination of the following conditions:

1. An activity that occurs on CLT property that differs from standard day-to-day operations
2. Involves any item(s) (decorations, catering, supplies, etc.) coming into the terminal building from anywhere else on or outside the Airport property and therefore requiring a security screening
3. Involves the distribution of goods, consumables, or other items
4. Includes any request(s) to change Security protocols
5. Includes any request(s) for facilities support (extra trash cans, trash pickup, tables, etc.)
6. Includes any request(s) to place event signage in a passenger-facing area that is outside of a reserved event space (e.g., Piedmont Conference Room)

**Foreign Aircraft Operator 1546 –** Operation of aircraft within the United States by a Foreign Air Carrier holding a permit whose employee, subcontractor, and subsidiaries' fingerprinting and adjudication will be completed by CLT under 1542 after the designated Authorized Signer has submitted a complete and accurate application.

**Laydown Yard -** A predetermined area authorized by a contractual or other written agreement between the airport or an airport tenant and a contractor authorizing use of said space to store raw materials and equipment for use on the airport. Laydown areas are not guaranteed and must be coordinated through the airport or tenant project manager.

**LEO** – Law Enforcement Officer.

**Local Interim Disqualifier** – Charges, arrests, and indictments that are potential disqualifiers. This includes warrants and indictments.

**IDMS** – Identity Management System, which is the software utilized to request and manage Access Media at CLT.

**Notice of Violation Review Board (NVRB) –** A Committee that reviews evidence and appeals and issues findings for security and conduct violations.

**Piggybacking** – The act of following someone through an access point without the person using their own Badge or Key.

**Prohibited Item –** Any item that is not allowed in the Sterile Area or on the aircraft, as listed in the carry-on standard list on the tsa.gov website. This term does not include Dangerous Weapon.

**Public Area –** Area normally accessible to the general public. Includes public portions of the terminal building, parking lots, and parking roadways.

**Restricted Areas –** Areas not open to the public and include all SIDA and Secured Areas, AOA, and non-public portions of the Sterile Area, to include the main terminal basement and loading dock area.

**Secured Area –** Portion of an airport, specified in the airport security program, in which certain security measures specified in Part 1542 of 49 CFR Chapter XII are carried out. This area is where aircraft operators and foreign air carriers that have a security program under Parts 1544 or 1546 of this chapter, enplane and deplane passengers as well as sort and load baggage, and any adjacent areas that are not separated by adequate security measures.

**Security Identification Display Area (SIDA) Area –** SIDA means a portion of an airport specified in the airport security program in which security measures specified in 49 CFR Part 1542 are carried out. This area includes the Secured Area and may include other areas of the airport.

**Security Threat Assessment (STA)** – A background check conducted by the TSA to determine that an individual does not pose a security threat.

**Sponsorship Letter –** A document establishing an entity's contractual relationship with CLT or an authorized Airport User. It also serves as a justification of the operational need for Access Media and may serve as authorization for the entity to establish its own Authorized Signer.

**Sterile Area –**Portion of an airport defined in the airport security program that provides passengers access to boarding aircraft and to which that access generally is controlled by TSA, or by an aircraft operator under Part 1544 of 49 CFR Chapter XII, or a foreign air carrier under Part 1546 of said chapter, through the screening of persons and property.

**Tailgating –** The act of driving a vehicle through a vehicular gate behind another vehicle without the driver using their own Badge to authorize access. Basically, piggybacking in a vehicle.

**Unescorted Access** – The authority granted by an Airport Operator, an Aircraft Operator, Foreign Air Carrier, or Airport Tenant under Parts 1542, 1544, or 1546 of 49 CFR Chapter XII, to individuals to gain entry to, and be present without an escort in, secured areas and SIDAs of airports.

**Vendor** – Companies that sell goods and/or provide customer support services for the operation of airport tenants (those with leaseholds) and may retain a leasehold or other instrument that ascribes to them the privileges usually found under a lease or exclusive area agreement. These do not include Air Carriers, Contractors, and Concessionaires, but may include Airport Tenants.

# 3 Compliance Requirements

All users of CLT must comply with these Security Standards, as well as applicable laws, regulations, directives, policies, and directives of CLT staff, TSA, Law Enforcement, and anyone tasked with enforcing the Airport Security Program while conducting business at CLT. The following outlines the various areas at CLT and what Access Media is required to access those areas, how to obtain Access Media, the responsibilities of Access Media holders, and the notice of violations and consequences of not complying with these standards. Such consequences may include, without limitation, the following:

a. Be denied future access to the Secured, Air Operations Area, SIDA, or Sterile Areas.
b. Have access privileges or CLT Badge suspended for up to 30 days.
c. Have access privileges or CLT Badge permanently revoked.
d. Be fined or otherwise penalized in accordance with applicable regulatory measures.
e. Have escort privileges suspended or revoked.
f. Have authorized signer privileges suspended or revoked.
g. In addition to CLT penalties related to security violations, employees, companies, contractors, and organizations may be subject to TSA penalties for violations of applicable Federal laws and regulations.

# 4 Procedures for Access to Restricted Areas

## 4.1 General Requirements for Access

### 4.1.1 The only persons authorized to enter restricted areas are:

a. Authorized and properly identified CLT personnel, tenants, tenant employees, contractors, and airline employees assigned duty or aviation activity or who have an operational need to be in a particular area;
b. Passengers who have properly submitted to screening and are entering to enplane or deplane an aircraft;
c. Persons under appropriate supervision or escort (see sections 4.1.2 and 7.7);
d. Persons having prior written CLT authorization; and
e. Properly identified FAA or DHS employees or representatives.

### 4.1.2 Visitor Passes

All unbadged personnel with a business need to access the Sterile Area are required to be issued a visitor pass or airline-issued gate pass, submit to TSA screening prior to entering the

Sterile Area, and remain under escort at all times while in the Sterile Area. Authorized Signers are responsible for reading and understanding the latest procedures related to this process via the Authorized Signer Portal. Authorized Signers will be responsible for determining which type of pass is needed. Airport-issued visitor passes must be requested through the Authorized Signer prior to 07:00 PM Eastern Time on the evening before the day the pass is needed.

Personnel with a business need to access the Sterile Area are permitted:

a. Up to 3 visitor passes within a 30-day period if they do not submit to the badging process.
b. Up to 30 visitor passes after the employee has been fingerprinted for badging.
c. Must be escorted at all times while in the Sterile Area.

Any exceptions to this policy must be requested by emailing: ASC@cltairport.com and avvisitorpasses@cltairport.com.

Individuals who enter under a visitor pass for reasons other than work must remain in the publicly accessible areas unless they are escorted by an individual with an ESCORT designation on their badge.

Individuals who committed a security violation are not eligible to receive visitor passes until they satisfy any imposed penalties. Individuals who received a notice of security violation that is pending adjudication for resolution is not eligible to receive a visitor pass. Additionally, individuals whose badge has expired, was lost, or is in any other way unavailable are prohibited from being issued a Visitor Pass.

Please note that exceeding the number of allowed visitor passes as described above, having access revoked due to a security violation, losing a badge, or having an expired badge does not permit unbadged personnel to be escorted through any other means. Doing so will be considered bypassing screening measures, which is considered a Tier 3 security violation, carrying the maximum penalty of permanent badge revocation.

## 4.2 Security Screening

### 4.2.1 Who Must be Screened

Aviation workers possessing airport-issued identification (ID) media and their Escorts are subject to screening/inspection for unauthorized weapons, explosives, and incendiaries. Non-compliance with the airport operator's aviation worker screening policy could result in penalties, which may include confiscation of their airport operator-issued ID media and/or revocation of unescorted access authority.

In addition, all persons desiring to enter the Secured Area, AOA, SIDA, or Sterile Area are subject to, and consent to, security screening, questioning, inspection, and search of their persons and accessible property as required by law and must comply with the system, measures, or procedures being applied to control access as defined in these rules. This includes Badge holders and those under escort. Screening and searches may be conducted randomly by the TSA or other appointed authority at any time a person is attempting to access or while in restricted areas. Compliance with inspections while at an access point or within the restricted area is mandatory. Inspections can include a search of your person, your outer coat and jacket, your accessible property, and your Badge. If an invalid Badge is presented, Prohibited Items, Dangerous Weapons, incendiaries, or explosives are found, or a person is believed to be otherwise unauthorized, the following will occur:

a. Access to the restricted area will be denied.
b. An attempt will be immediately reported to the Airport Operations Center at 704-359-4012, and both individuals reporting the incident and those in violation must stay on-site until Airport Security arrives.
c. During the call, a brief description of the violating individual and their location will be provided.
d. An attempt to keep the violating individual in sight until assistance arrives will be made.
e. Violators may be cited as appropriate based upon the facts of the specific situation.
f. If an individual is determined to be unauthorized, they may be detained or removed by the Aviation Director or his designee, CMPD, or the TSA.

**Note:** Individuals are considered submitted to screening upon getting in line to or attempting to enter the restricted area and may not leave once they have entered the line until screening is complete. Additionally, please review section 7.2 for more information related to screening requirements for employees.

### 4.2.2 CLT Issued Badge Description and Authorization

CLT issues Badges that indicate the areas to which the individual has unescorted access and other endorsements and privileges. These privileges are identified through colors and icons as described below.

| Color | Area | Access (NOTE: "Access" refers to the different security areas the badge can be utilized in. Each badge will have specific permissions added to support necessary access for the employee's job function. |
|---|---|---|
| | RED Sterile Area Only | Must gain access to the Sterile Area through a TSA screening checkpoint only |
| | Green - CLT Secured/Cargo Areas/GA | All Areas of CLT |
| | Orange - CLT GA/South Cargo Areas | AOA south of taxiway C8, the FBO east of runway 18L/36R, and Sterile Areas |
| | Yellow- Contractor | Allowed to be in all areas of CLT, issued to Contractors |
| | Gray - CLT Public Areas | Areas prior to security checkpoints only. Issued to certain public-side entities with contractual relationships with the City of Charlotte. |
| | Blue - Government | All areas of CLT |
| Endorsements by Badge: ESCORT – Escort Privileges; DR – AOA Driving privileges, DR-E – Vehicular Escort Privilege; Customs Seal – Access to Federal Inspection Station area; **AEOC/ICP -** authorization to enter the AEOC or emergency scene.; approval required. | | |

## 4.3 Additional Airport-Approved Identification Media

Some individuals are allowed to access the restricted areas with identification issued by other agencies. Such identification is referred to as Airport Approved Identification and is outlined below.

a. FAA Aviation Safety Inspector ID. FAA Aviation Safety Inspectors possessing FAA Form 110A have unescorted access to those portions of the SIDA in which it is necessary for them to conduct their assigned duties of inspection. FAA Aviation Safety Inspectors must have Form 110A in their possession at all times. There are some restrictions on the Use of Form 110A. While Form 110A is considered an official identification medium in secured areas, it does not provide the inspector access to areas that are not being inspected. Access to other secured areas must be gained through local airport procedures.

b. Air Carrier ID. Flight crew members who are in uniform and wearing their air carrier-issued identification medium readily visible at waist level or above may access the

following portions of the Secured Area: The immediate vicinity of the aircraft to which the flight crew is assigned; The flight crew operations/flight office, or its equivalent; and points in between as authorized by CLT.

c. TSA Inspection Authority. The TSA may enter and be present within Secured Areas, the AOA, and SIDA without access media or identification media issued or approved by an Airport Operator or Aircraft Operator in order to inspect or test compliance or perform other such duties as TSA may direct pursuant to applicable federal law.

# 5 CLT Badge Procedures

The following sections outline the steps required for an Airport User to request and an individual to receive a Badge at CLT. This information, as well as other helpful documentation, may also be found at www.cltairport.com/business/credentialing.

## 5.1 Credentialing Services

As a general rule, the Credentialing office follows the information located on their website, cltairport.com/business/credentialing, or for further information, email avbadging@cltairport.com.

## 5.2 Determination of Eligibility for Issuance of a CLT Badge

### 5.2.1 TSA Authorization and Requirements

Before CLT can issue a Badge to a new employee, TSA must complete a Security Threat Assessment ("STA") and authorize the issuance of a Badge to that individual. If approved, CLT will issue a CLT Badge to the individual, allowing access to those portions of CLT where the employee has an operational need and is authorized to be.

Further, CLT must ensure that no individual is granted unescorted access authority unless the individual has undergone a fingerprint-based Criminal History Records Check (CHRC) that does not disclose a disqualifying criminal offense.

**Exception:** Government Employees of federal, state, and local government agencies who, as a condition of their employment, have been subjected to an employment investigation that includes a fingerprint-based criminal history background check are not required to submit to a second fingerprint check. Their governmental agency identification badges will be accepted as verification that a prior employment check has been completed.

### 5.2.2 ASC Determination

The ASC, or his/her designee, will evaluate each request for a CLT Badge to determine if there is an operational need for the applicant to have access to a restricted or secured area on a regular basis. This determination is for access privileges only, as the ASC or his or her designee does not make employment decisions.

## 5.3 Employer or Sponsoring Company Responsibilities

### 5.3.1 Compliance Agreement and Authorized Signer Letters

Each authorizing Airport Tenant and Air Carrier must submit a signed letter stating their agreed-upon compliance with the credentialing process as required based on their designation as an Airport Operator 1542 (or under that process), Aircraft Operator 1544, or Foreign Aircraft Operator 1546. The letters:

a. Authorize a direct employee or a sponsored company employee to proceed with the fingerprint process conducted by CLT or the Air Carriers; and

b. Certifies that there is an operational need for applicants to have unescorted access. For convenience, sample letters are available on the Credentialing webpage: www.cltairport.com/business/credentialing.

### 5.3.2 Ensure Compliance with Application Process

Companies are required to ensure that their employees, including contract employees, submit to the background clearance application process, which includes a CHRC and STA. CLT does not accept CHRC/STA information from other airports.

### 5.3.3 Background Checks

To determine badging eligibility, TSA requires all applicants to pass both the CHRC and STA. Some Air Carriers (1544 companies) are permitted to conduct the CHRC independently but are required to provide certification that the applicant is Rap Back enrolled. Such certification shall include the Offense Cycle Number (OCN) and date of fingerprinting. Air Carriers will be held responsible for ensuring these checks are completed in accordance with federal regulations and will immediately notify Credentialing when/if a badge holder is disenrolled from Rap Back. The ASC may not require the Aircraft Operator to provide a copy of the criminal history record check completed by the Aircraft Operator.

### 5.3.4 Authorized Signer (AS) Designation

Airport Tenants and Air Carriers may designate authorized signers to request Access Media if they have a direct business relationship with or lease space at CLT. All other companies must be sponsored by an Airport Tenant, or Air Carrier authorized to request Access Media. The AS is

the primary point of contact for Airport Security matters, and CLT requires a minimum of two (2) up to four (4) AS designations per Airport Tenant or Air Carrier with less than 500 employees. Exceptions can be made on a case-by-case basis with operational justification and ASC approval.

To qualify as an AS, the individual must:

a. Hold a valid Badge in good standing at CLT;
b. Attend CLT AS training once every 12 months, for which they must register by emailing avbadging@cltairport.com.
c. Agree to meet all AS responsibilities

**Note:** Authorized signers are not allowed to sign an application for their own badge.

## 5.4 Authorized Signer Badge Application Responsibilities.

### 5.4.1 General Requirements

Once all requirements to become an AS are met, the AS will be granted access to the AS Web Portal, which acts as the Airport User's interface with IDMS to submit applications and initiate new, renewal, and Badge change requests. The login authorization for the Portal is unique to the AS, and the login information must be safeguarded **NOTE:** Failure to protect or sharing the AS portal login information is akin to loaning the Badge and is a severe violation (Tier 3) that will result in ***permanent Badge revocation*** and entry into the Centralized Revocation Database ("CRD") that is maintained by the DHS, for all the parties involved.

To ensure an applicant can be processed as efficiently as possible, Authorized Signers must:

a. Ensure the applications are complete based upon the requirements for the applicable operator designation (Airport Operator 1542, Aircraft Operator 1544, or Foreign Aircraft Operator).
b. View the forms of identification presented by the applicant and ensure they meet regulatory requirements for determining identity and work authorization found on the United States Citizenship and Immigration Services website; https://www.uscis.gov/i-9
c. Only submit legible, valid, non-expired identification. **NOTE:** A laminated Social Security Card will not be accepted as a form of identification.
d. Submit accurate applicant information, paying particular attention to biographical data; legal name, date of birth, and SSN. Country of birth and citizenship errors are of particular concern and will result in application rejection and may be referred to TSA for further investigation.
e. Ensure the applicant has acknowledged the Disqualifying Crimes and Disclosure Statements and reviewed the CLT Security Standards via a link provided by the Web Portal and delivered to the applicant's email on file. **NOTE:** This acknowledgment cannot

be done by the AS. It is considered falsification of records if the AS completes this for the applicant, and it will result in permanent revocation of the AS Badge.

f. Ensure they are the only individual(s) completing background clearance applications via a secure web portal, requesting CLT access media and access changes, as well as addressing access control issues that may arise. **NOTE:** This responsibility may not be delegated to non-AS personnel.
g. Schedule credentialing appointments through the scheduling system provided by CLT.
h. Only submit applications for those employees within their own company/department or their sponsored subcontractors.

Applications will not continue with the credentialing process, and the applicant will be turned away if any of the above steps are not met. ASs are required to comply with the Security Standards that govern the credentialing process. AS is also responsible for safeguarding their portal login information, returning Keys, Security Keys, and Badges, and deactivating Badges immediately when lost/stolen or the employee otherwise separates from the company. Failure to comply with the guidelines may result in suspension, loss of AS privileges, and/or permanent revocation of the Badge, as further described in Section 9.2 below.

### 5.4.2 Fingerprint and Renewal Applications

Prior to being fingerprinted and upon renewal, each applicant will be required to complete and acknowledge the following statements via the Authorized Signer Web Portal:

a. A statement that the individual signing the application does not have a conviction for a disqualifying criminal offense.
b. A statement informing the individual that Federal Regulations under 49 C.F.R. § 1542.209 (1) impose a continuing obligation to disclose to the Airport within 24 hours if that individual is convicted of any Disqualifying Crime that occurs while he/she has unescorted access authority.
c. A statement confirming that the information the applicant has provided is true, complete, and correct is provided in good faith and that a knowing and willful false statement on the application can be punished by fine, imprisonment, or both.

### 5.4.3 Access Requests and Changes

CLT assigns individuals to door clearance groups based on the position held within an organization. These clearance groups are assigned when the Badge is printed. From time to time, changes to clearances are necessary and are usually due to the following:

a. Organizational change requiring additional doors or access points.
b. Positional changes, promotions, demotions, or transfers.
c. Temporary project.

Ideally, many of the changes will be captured during the badging process; however, when a change is necessary for an access group, individual, or projects, Authorized Signers can either email CLTAccess@cltairport.com or fill out an online CLT Onboarding and Change form that can be found on www.cltairport.com/business/credentialing. Any subcontractors needing a change in access must request this change through the primary contractor. Please allow up to five business days for the change to take effect.

## 5.5 Applicant Responsibilities

Employees requesting unescorted access to restricted areas of CLT will:

a. Submit to a Security Threat Assessment
b. Submit to a fingerprint-based Criminal History Records Check (CHRC)
c. Complete Regulatory Training as applicable
d. Complete the AOA driver's training course for the operation of vehicles in the AOA in accordance with FAR 139 if required to operate a vehicle in the AOA, and
e. Comply with all other CLT and/or TSA requests and/or requirements.

**Note:** Employees must have a Badge for each of their employers at CLT.

## 5.6 Badge Issuance

### 5.6.1 Conditions

An individual may be issued a Badge unless the credentialing process identifies a disqualifying criminal offense or unresolved legal issues.

a. **Disqualifying Criminal Offenses.** An individual has a disqualifying criminal offense if the individual has been convicted or found not guilty by reason of insanity of any of the Disqualifying Crimes in any jurisdiction during the ten (10) years before the date of the individual's application for unescorted access authority, or while the individual has unescorted access authority.
b. **Local Interim Disqualifier.** Applicants and/or Badge holders that have an arrest, charge, or indictment that potentially involves a disqualifying offense, as well as Applicants or Badge holders that have active warrants, cannot have or be granted

unescorted access, receive a visitor's pass or be under escort until the warrant is cleared and/or a court disposition is provided in accordance with 49 C.F.R. 1542.209, and other applicable TSA regulations and directives if the disposition did not result in a conviction or a finding of not guilty by reason of insanity of one of the Disqualifying Crimes unescorted access may be authorized.

c. **Centralized Revocation database (CRD) Entries.** Badge holders and applicants who have been entered into the DHS CRD by another airport are not eligible for unescorted access, a visitor pass, or escort until their CRD entry has expired. Additionally, persons permanently revoked by CLT airport will be ineligible for any future unescorted access considerations at CLT airport. This will also include visitor passes and an escort.

d. **Determination of Arrest Status.** When a CHRC reveals that an individual seeking unescorted access authority who is not covered by an Air Carrier certification has been arrested for any criminal offense, without indicating a disposition, the ASC or his/her designee must investigate the arrest to determine whether it involves a Disqualifying Crime. During the investigation, no Badge may be issued or held by such an individual until the disposition is provided. If the disposition did not result in a conviction or a finding of not guilty by reason of insanity of one of the Disqualifying Crimes, unescorted access may be authorized.

CLT maintains the discretion to restrict, terminate, or deny unescorted access authority when necessary to maintain the integrity of the Airport Security Program.

**Note:** The Airport may perform subsequent recurrent CHRCs on Badge holders with access to Secured Areas who are required to complete a CHRC by federal regulations.

### 5.6.2 Notification of Disqualification

The ASC will do the following prior to making a final decision to deny unescorted access to an individual because of a disqualifying criminal offense:

a. Inform the applicant that the FBI criminal record revealed information that would disqualify him/her from receiving a CLT ID Badge or restrict his/her unescorted access authority.
b. Provide the applicant with a copy of the FBI record, if requested in writing.
c. Deny unescorted access authority if an applicant does not notify the Airport of intent to correct the information revealed in the CHRC or provide documentation to refute or correct the information within 30 days of receipt of the Disqualification Letter.

### 5.6.3 Corrective Action by Applicant

An applicant has thirty (30) days from receipt of the Disqualification letter to notify the Airport in writing of the intention to correct or provide case disposition information to assist the Airport in

making a final decision. An applicant must provide a revised/corrected FBI Criminal Investigation Record or a certified true copy of the disposition information from the appropriate municipal or government court within 30 days of receipt of the disqualifying letter.

### 5.6.4 Disqualifying Criminal Offenses for Current Badge Holders

If information becomes available to Airport Users indicating that an individual with unescorted access has a Disqualifying Crime, the Airport User must report the offense to the Credentialing Office or ASC at 704-359-4010 within twenty-four (24) hours of the conviction or finding of not guilty by reason of insanity;

a. The ASC or designee must determine the status of the conviction; and
b. If a Disqualifying Crime is confirmed, the ASC or designee shall immediately revoke any unescorted access authority.

### 5.6.5 Procedures for Obtaining Copies of CHRC Results

Requests for copies of the results of a Criminal History Records Check must be submitted in writing to:

CLT Fingerprint Copy Request
Attention: CLT Credentialing Office
PO Box 19066
Charlotte, NC 28219

Employees must include a legible photocopy of a government-issued photo identification with their request. Replies will be sent to the email address on record.

### 5.6.6 Limitations on Dissemination of Results of CHRC

The ASC or designee will not disseminate the results of the CHRC to anyone other than:

a. The individual to whom the results pertain or that individual's authorized representative;
b. Authorized officials of other Airport Operators who are determining whether to grant unescorted access to the individual under this part;
c. Aircraft operators who are determining whether to grant unescorted access to the individual or authorize the individual to perform screening functions; and/or
d. Others designated or authorized by the TSA.

### 5.6.7 Sharing CHRC/STA data

CLT airport does not participate in the sharing of or accept CHRC/STA information with or from other airports.

### 5.6.8 Recordkeeping

The ASC or his/her designee will maintain and control the following information until 180 days after the termination of an individual's unescorted access authority:

a. Employment history investigation files, including the criminal history results portion or appropriate certifications for investigations conducted before December 6, 2001;
b. Certifications provided by Air Carriers on or after December 6, 2001;
c. Badging information including social security number (SSN); date of birth; description/physical characteristics including height, weight, the color of hair and eyes, sex, and ethnic origin; home address; driver's license number (if applicable); Badge issue date; criminal history record information;
d. Signed STA application and any communications with the TSA regarding the individual's application.

#### 5.6.9 Confidentiality

CLT will maintain all records in compliance with all legal and regulatory requirements in order to protect the confidentiality of the individual's personal identifying information.

## 6 Airport User and AS Responsibilities

Airport Users or their designated AS are a key layer to the overall security at CLT and, as such, are responsible for additional security measures in addition to those required of a Badge Holder, and all such individuals must be active Badge Holders themselves. These responsibilities include, without limitation:

#### 6.1.1 Security, Safety, and Passenger Handling Program

Air Carriers must have a written, TSA-approved security, safety, and passenger handling program.

#### 6.1.2 Dissemination of Information to Employees

All Airport Users are responsible for disseminating airport security rules, regulations, and procedures to their employees, as well as ensuring their employees have the ability to comply. Likewise, any updates or changes shall be disseminated to employees by their respective employers, and the dissemination of the information is subject to certification upon request of CLT.

a. **Security Doors**. Airport Users shall be responsible for security doors located in their leased areas. Airport Users who fail to control unauthorized access into the Secured Area or AOA through doors located in tenant-leased space may be subject to monetary fines and may be subject to TSA civil penalties.
b. **Disqualifying Offenses for Current Badge Holders.** Airport Users and Authorized Signers are obligated to notify the CLT Credentialing Office or the ASC immediately upon becoming aware that one of their Badge holders has a Disqualifying Crime.

c. **Seeking Prior Written Approval Before Making Modifications**. Airport Users must seek written approval and authorization before making any modifications to their leased space, including making changes to security boundaries, fencing, access control systems, or any audio/visual media/surveillance equipment. Airport Users seeking that approval must agree to share the audio/visual feeds of any new equipment in a format that is acceptable to the CLT. These requests must be made no later than 60 days before the intended modification through the tenant modification process.

d. **Events in Restricted Areas** - Airport Users must seek written approval and authorization before holding events in the Restricted Areas. These requests must be made to the ASC or their designee no later than 60 days before the date of the event.

e. **Concessionaire Prohibited Items and Knife Audits**. Concessionaire shall not offer for sale any Prohibited Item and must conduct and document a knife audit at the beginning of each shift.

f. **Deliveries, Merchandise, or Consumables** – intended for sale, or distribution to the public in the Sterile Area must be inspected according to established procedures at the Loading Docks, field gates, or other locations approved in writing by the ASC. The request for an alternate inspection location must be submitted to the ASC a minimum of 72 hours before the intended delivery.

## 6.2 General Accountability Procedures.

Airport Users and their designated AS are accountable for the Badges issued through the AS. Each Airport User, through its AS, is required to:

a. Provide Credentialing with an authorized/certified signature letter to be kept on file.

b. Keep a record of its active authorized Badge holders and the corresponding expiration date for each Badge.

c. Immediately deactivate the Badge in the Authorized Signer portal of Airport ICE system (AS Portal), or notify the Credentialing office at 704-359-4010 during business hours or 704-359-4012 after business hours, of a change in an employee's status, i.e., extended sick leave, reassignment, suspension, termination, abandonment of position, etc.

### 6.2.1 Badge Status.

The AS is responsible for ensuring each Badge is assigned the proper status in the IDMS. Airport IDMS will accept the following Badge status categories:

a. **Active:** is a Badge that is issued to an employee who has been granted unescorted access to restricted areas of the airport for official business only.

b. **Revoked:** is used when an employee's need and/or employment/relationship with a

company or organization has terminated, and unescorted access is no longer needed. Revoked Badges cannot be reinstated and will require the applicant to start from the beginning of the badging process.

c. **Lost:** is used when the employee loses a Badge and will initiate a replacement.
d. **Suspended:** is used to deactivate a Badge for a temporary period, off-site for an extended period, medical leave, Leave of absence, or military deployment. Suspended Badges will require a completed Badge Reactivation and Replacement form to reactivate. Suspended badges must be returned to the Credentialing office within 48 hours of deactivation.
e. **Expired:** is a Badge that has not been renewed prior to midnight on the expiration date displayed on the Badge. An expired Badge of more than 30 days will require an applicant to start from the beginning of the badging process. Individuals whose badge has expired are not eligible for visitor passes or to be escorted into the Restricted Areas. Individuals whose badge has expired may not attempt to use other access media or physical keys to enter secured or restricted areas.

### 6.2.2 Lost, Stolen, or Destroyed Access Media.

Lost or unreturned Access Media present an increased security risk in the airport environment that requires additional measures to enhance their accountability and encourage their prompt return. Employees cannot have more than three unaccounted-for Access Media at any time. Additional badges will not be issued until at least one of the three unaccounted-for Access Media has been returned or has expired, and the associated fee has been paid. Unaccounted for Access Media include: lost, stolen, revoked, unreturned, and suspended not returned Badges or keys.

If any Access Media is lost, stolen, or destroyed, the badge holder must immediately notify their Authorized Signer or Credentialing Office at 704-359-4010 during business hours or Airport Operations Center 704-359-4012 after hours. Lost, stolen, or destroyed Access Media reports may be made by telephone, seven days a week, 24 hours a day. Upon notification of a lost, stolen, destroyed, or unaccounted-for Access Media, CLT will terminate all access associated with that Access Media and note the Access Media record accordingly. Authorized signers can also immediately deactivate badges via the authorized signer portal 24/7 when unescorted access is no longer required.

### 6.2.3 Lost or Stolen Access Media Limitation.

Lost or stolen Access Media can only be reported for active and current employees, not for employees who resigned, transferred, terminated, or otherwise left employment at the Airport and failed to return the CLT ID Badge or keys. Badges and keys belonging to former employees must be reported as terminated or unaccounted for.

### 6.2.4 Reapplication for CLT Badge.

A Badge holder whose card has been lost, stolen, or destroyed due to negligence must:

a. Not have more than three lost, stolen, or unaccounted for Badges at any time.
b. Contact the AS who will complete out an endorsement update Badge Reactivation and Replacement form and submit it to Credentialing.
c. Wait a minimum of 24-hours and come to Credentialing Office for re-issuance.
d. Remit payment for the lost Badge:
    i. $135 for the first lost Badge
    ii. $235 for the second lost Badge
    iii. $335 for the third lost Badge.

The penalty cannot be billed to the employer and must be paid by Credit or Debit Card in person when the Badge is being re-issued.

An applicant is not eligible to receive a replacement after losing three Badges within thirty six (36) months and may not receive subsequent Badges for any company until a lost Badge is returned or the fee paid.

### 6.2.5 Mandatory Return of Badges

Whenever employment status is terminated, suspended, or the Badge holder transfers to another station, or there is no longer an operational need for a Badge holder to have access to the AOA, SIDA, Secured, or Sterile Areas, the CLT Identification Badge must be deactivated and returned to the CLT ID Badging Office by the employer or employee.

### 6.2.6 Penalty for Failure to Return Badges

The employers will be charged $100 for any employee's single area Badge and $200 for multiple area Badge not returned within 48-hours of the Badge expiration or the employee's separation. Any applicant who has an unaccounted-for Badge in their record will need to return the Badge or pay the lost badge fee before being issued a new Badge. The lost Badge fees are listed above.

Airport Users with a pattern of not returning Badges will be required to:

a. Enter into a Corrective Action Plan (CAP);
b. Pay any fines levied.

### 6.2.7 Confiscation of Badges

CLT Badges are the sole property of the Airport, and it is the Airport User's responsibility, through their designated AS, to ensure their Badge is returned upon expiration, an employee's separation from employment, or upon demand by CLT or the employer. A Badge may be confiscated for the following reasons:

a. **Penalty for Violation of Rules and Regulations.** CLT may restrict access privileges and confiscate Airport Identification Badges of Badge holders who violate the CLT Security Standards and other Airport rules and regulations. Failure to affirmatively act when required to (such as to report a suspicious activity or situation as prescribed in Section 7.6) may also constitute a violation of rules and regulations. Violators may also receive a monetary fine and be required to re-attend the SIDA Training Class.

b. **Penalty for Inappropriate Conduct on Airport Premises.** CLT reserves the right to restrict access privileges and confiscate Badges of Badge holders who engage in inappropriate conduct, which includes but is not limited to using offensive or threatening language and/or gestures; refusing to cooperate with law enforcement, CLT staff, TSA, or other individuals charged with implementing the provisions of the ASP, or other rules and regulations of CLT; tampering or interfering with the Airport's access control system; interrupting or disrupting airport operations, or damaging airport property. Note: Disseminating or releasing, without authorization, either security sensitive information ("SSI") as defined in 49 CFR Part 1520, or other information that would not have otherwise been known or observable to the general public that has the potential to impede an investigation or adversely impact operations may be considered inappropriate conduct, depending on the totality of the circumstances.

c. **Confiscation of Badge for Conviction of Crimes Committed on Airport Property**. CLT will permanently revoke the Badge and all access privileges of any Badge holder who is convicted of a misdemeanor or felony committed on airport property.

d. **Confiscation of Badge for Conviction of Disqualifying Crime.** Badge holders are obligated to report to the ASC or his/her designee within 24 hours if they have been convicted, plead no contest, or found not guilty by reason of insanity of any of the Disqualifying Crimes listed in Appendix 2. Their Badges will be deactivated and confiscated immediately.

When a Badge has been confiscated, the ASC or his/her designee will determine the reauthorization of the individual's access privileges pending the violator's completion of SIDA training, re-issuance of Employer/Company justification for clearance, and timely payment of any fines incurred by CLT.

### 6.2.8 CLT's Responsibilities and Right to Audit

CLT is responsible for the control, accountability, and issuance of CLT Access Media. To accomplish these responsibilities, CLT reserves the right to audit Airport Users' Access Media records at any time, without prior authorization or notification. The ASC or his/her designee will conduct an audit of all active Access Media that allow access to the AOA, Sterile and/or Secure Areas annually, randomly or whenever there is a reason to suspect that the CLT Access Media

Identification System has been compromised; The audit will be initiated and completed in the Authorized Signer portal, or manually, and with instructions to include a due date.

CLT is also responsible for the control and accountability of Prohibited Items. Audits will be conducted on a random basis to validate the Concessionaire's ability to maintain control and accountability of Prohibited Items and knives used in the Sterile area. In addition, the concessions audit will validate that Concessionaires are not offering Prohibited Items for sale or carrying them in their inventory.

## 6.3 Contractor and Construction Responsibilities

### 6.3.1 Contractor Credentialing

All contracted companies with a direct business relationship with CLT or an Airport Tenant will need to be either signed for by CLT, the department for which they are contracting (e.g., Bravo Plumbing for CLT Facilities will need to be signed for by the Facilities Department), or an Airport Tenant. Under certain circumstances, as determined by CLT, these companies will enter into a sponsored relationship with CLT or an Airport Tenant and establish their own AS for all credentialing needs under this sponsorship. These sponsorships must be approved in advance by filing the sponsorship letter available on the Credentialing web page at https://www.cltairport.com/business/credentialing/.

The approval of a sponsorship letter is intended to enhance efficiencies in the Credentialing process; however, a sponsorship approval can be revoked at any time by CLT airport when either the sponsor or the sponsored company does not meet Authorized Signer responsibilities, including general negligence and badge accountability concerns. Once approved, this letter will remain on file in Credentialing until expiration or revocation.

The renewal of the sponsorship letter is the responsibility of both parties. If the sponsored relationship expires, the sponsored company will lose access and credentialing privileges.

### 6.3.2 Sub-contractor Relationship

Contractors with their own AS are responsible for all credentialing functions of all of their sub-contractors, as well as all their and their sub-contractors' security posture, including familiarity and compliance with these Security Standards and all rules and regulations at CLT.

All contractors' and sub-contractors' Badges are issued for a specific project or contract and cannot be used for any other purpose. When a contractor or subcontractor begins a new project or enters into a new sponsored relationship, they must obtain new Access Media for the new project or relationship.

### 6.3.3 Construction Areas and Equipment Storage

CLT maintains a clear zone of 10 feet on either side of the perimeter fence or any laydown yard fence. If access portals are preset, Laydown yards and any construction zones must be secured with a lock and key when unattended, regardless of the location of the construction site. Temporary construction walls and laydown areas with access portals must be cored to the latest specifications set forth by the CLT Locksmith and be secured at any time personnel are not actively transitioning through the door. Please refer to the Tenant/Concession Design Standards for the latest requirements related to temporary construction walls. All designs for temporary construction areas must be vetted and approved by CLT prior to implementing any such measure.

Storage containers or other media are not permitted in the Sterile Area by contractors without express written permission from CLT Security. Storage containers in approved areas must display an inventory of all prohibited items necessary for the job function.

### 6.3.4 Sponsorship

As mentioned above, sub-contracted companies without a direct business relationship with CLT or an Airport Tenant will need to be either signed for by the prime company or have an approved sponsorship letter on company letterhead on file with Credentialing. An example of a Sponsorship letter can be found on the Credentialing web page at; https://www.cltairport.com/business/credentialing/. The approval of a sponsorship letter is intended to enhance efficiencies in the Credentialing process; however, a sponsorship approval can be revoked at any time by CLT airport when either the sponsor or the sponsored company does not meet Authorized Signer responsibilities, including general negligence and badge accountability concerns.

## 6.4 Concessionaire Requirements

### 6.4.1 Access through checkpoints

All concessionaires are required to enter the Sterile Area through at a TSA security screening checkpoint.

### 6.4.2 Accountability for Knives and Prohibited Items

Concessionaires must keep an inventory of all knives used for food preparation and provide photo documentation of the items to the ASC. Any changes to the inventory must be reported to the ASC at asc@cltairport.com as soon as practicable and must be followed up with updated photo documentation within two business days.

Additionally, the knives must be tethered and kept from public access. They must be audited at the end of each shift. Any knives discovered missing must be reported to the ASC immediately. The concessionaire is required to keep the audit logs for a minimum of 30 days. These logs must be available for review by CLT and the TSA.

The requirements for the inventory, accountability of knives, and the phone number for reporting the missing knives must be posted in each area where concessionaires use the knives.

### 6.5 Airport User Access Control

Any modifications to Airport User spaces, including access control or CCTV coverage, must be requested through a Tenant Modification Agreement (TMA) process. Information on the TMA process is included in the Tenant Handbook available on the Tenant HUB.

## 7 Badge Holder Responsibilities

As a Badge holder at CLT, you are also another important layer to the overall security of the Airport. For that reason, there are responsibilities that come with the privilege of having a Badge. Failure to comply with these responsibilities can lead to an individual being cited. Such notice of violation can lead to suspension or even permanent revocation of the Badge. Where non-compliance could lead to permanent revocation, it is noted within the section describing the specific Badge holder's responsibility.

### 7.1 CLT Badge Display

All individuals requiring unescorted access to the Secured Area of CLT must wear their CLT Badges above the waist level, prominently displayed and readily visible on their outer clothing. Badge holders may not alter the appearance of the Badge in any way, including by covering up the picture or applying or wearing tenant ID badges, objects, stickers other than those authorized by the Airport, or other encumbrance over the Badge. Badge holders must immediately have the Badge replaced if it is damaged in any way, i.e., the Badge holder's name, Badge holder's picture, company name, or Badge expiration date becomes indistinguishable, or the Badge is torn or split in any way.

## 7.2 Proper Use of CLT Access Media

Rights to Access Media are a privilege, and use of such must always be in compliance with the following:

a. **Access Media Must be Used for the Purpose Issued.** No person may use, allow to be used, or cause to be used, any airport-issued or airport-approved Access Medium or identification medium that authorizes the access, presence, or movement of persons or vehicles in Secured Area, Air Operations Area, or SIDA in a manner other than that for which it was issued by the Airport unless otherwise approved by the ASC.

b. **Use of Another Person's Access Media Prohibited**. Badge holders are prohibited from using another person's Badge or providing their Badge to any other person for the purpose of unescorted access to a restricted or secured area. **NOTE:** Violation of this section will result in permanent revocation of the Badge of both parties.

c. **Access Media Must be Valid**. Badge holders are responsible for renewing their Badges before they expire and may not use or attempt to use an expired or otherwise invalid Badge to access the Restricted Area.

d. **Access Media for Use during Designated Work Hours for Job-Related Purposes**. Badge holders may only access the Restricted Areas during designated work hours and/or for job-related purposes unless approved by the ASC. For approved entry outside of designated work hours, the employees are required to enter the Restricted Areas through the security screening checkpoint unless all the screening checkpoints are closed at the time.

e. **By-Passing Required Security Measures.** All established security measures, including those in place to control access (such as, but not limited to, access-controlled doors, automated exit lanes, and vehicle access gates), conduct screening activities, and prevent the introduction of unauthorized items or personnel into restricted areas, shall not be bypassed. Examples of bypassing required screening measures include, but are not limited to:

- Utilizing access points to intentionally bypass random or continuous employee inspections.
- Employees with active Badges who fail to display them and attempt to enter a restricted area under escort.
- Badge holders traveling on commercial flights that use CLT Access Media to bypass the TSA Passenger Screening Checkpoint (this includes presenting a SIDA Badge at the TSA Screening Checkpoint Employee Lanes).
- Concessionaire employees entering the Sterile Area by any other means than the TSA Screening Checkpoint

- Using flight privileges to enter the Sterile Area in the absence of a valid Badge, or introducing a passenger's luggage into the Sterile Area through portals other than a screening checkpoint..
- Any other method utilized to intentionally gain access to restricted areas or otherwise defeat access control and/or inspection measures, including instances where such methods are used to grant access with an expired, inactive, or malfunctioning Badge (Note: The ASC reserves the right to evaluate each incident of alleged security measure bypassing to determine if the facts warrant a violation of this section).

**NOTE:** Violation of this section will result in permanent revocation of the Badge.

f. **Multiple companies.** Employees who work for multiple companies are required to access the airport with the Badge and also display the Badge for the employer for which they are currently on site. If any employee completes a shift for one company and is reporting to work for another, the employee must exit and re-enter the restricted areas of CLT using the second employer's sponsored Badge.

g. **Random screening and searches.** Employees are subject to random screening and searches by the TSA, CLT Security Operations, or other appointed authority at any time while attempting to access or while in Restricted Areas. Compliance with these inspections is mandatory, and avoidance by changing the intended entry point is not allowed. **NOTE:** Such avoidance will result in permanent revocation of the Badge.

h. **Copying, reproduction of Access Media -** It is strictly prohibited to provide false information to obtain, copy, reproduce, replicate, or duplicate CLT Access Media, application, or documentation for Credentialing purposes, and/or conduct any other fraud.

i. **Prohibition to Use Key Bypass –** It is prohibited to use a key on doors that are equipped with a functioning ID card-based access control system, unless approved by the ASC. **NOTE:** Using a key on such a door without permission will result in permanent revocation of the Badge.

## 7.3 Prohibited Items in Restricted Areas of the Airport

Prohibited Items are not allowed in the Secured Area, Sterile Area, or SIDA unless those items are necessary for the performance of a job. A Dangerous Weapon is never allowed unless the Badge holder is an LEO or other individual authorized by the TSA or ASC. **NOTE:** Introducing or attempting to introduce a Dangerous Weapon will result in a ***permanent revocation*** and entry

into the Centralized Revocation Database (CRD). A Badge holder or other Airport User is not allowed to introduce Prohibited Items not necessary in the performance of a job or leave any Prohibited Item unattended or unsecured in a Secured Area, Sterile Area, or SIDA of CLT.

The Prohibited Items list can be found by visiting www.tsa.gov *(Carry on Standard)*

### 7.3.1 Prohibited Items Necessary for the Performance of Job Duties.

Anyone in possession of Prohibited Item(s) required for the performance of duties entering a restricted area must:

a. Have a written inventory of the items.
b. Ensure the item(s) are required for the job they are currently performing.
c. Ensure control and accountability of the item(s) are maintained 100% of the time.
d. Ensure items(s) are locked and secured or in sight of the person when not in use.
e. Ensure items are stored in an area secured with a lock.
f. Violations of security procedures identified during a concessions/knife audit or as otherwise discovered related to failure to properly have and secure Prohibited Items will be documented with a security notice of violation.

See section 6.4.2 for rules governing the use of prohibited items by concessionaires.

### 7.3.2 Dangerous Weapons, incendiary, ammunition violation

No persons, except authorized law enforcement or other individuals authorized by the Transportation Security Administration or Airport Security Coordinator, may possess any dangerous weapons, incendiaries, or explosives in the Restricted Areas of CLT.

## 7.4 Securing an Access Point

Badge holders who use an access point (doors including elevator doors, or gates) must prevent unauthorized access, ensure they are securely closed behind them and ensure security integrity is maintained at all times.

**Note:** Badge holders who gain access to a Restricted Area via an elevator must ensure that each unescorted person on the elevator swipes his/her own CLT Badge and is signaled a green light on the card reader before proceeding.

In these cases, those who allow the action and those who fail to act in compliance with this section will be subject to a security notice of violation.

The following situations and failures to secure an access point will result in penalties:

a. **Leaving an access point unsecured and unattended –** Assuring to get a green light on the card reader before proceeding, badge holders must ensure that all

doors, including elevator doors, or gates they open are securely closed behind them and must not allow anyone else to enter behind them without that person utilizing his/her own CLT-issued Access Media. In case of an alarm, the badge holder must resolve the alarm or remain at the door/gate and prevent access by others until Airport Operations personnel arrive and take control of the door/gate.

b. **Malfunction of Access Point -** Badge holders who use, or attempt to use, his/her CLT SIDA badge or security key(s) to open an access-controlled door or gate and find a malfunction of the alarm, or the locking mechanism, that will reduce or negate control, must report the malfunction to the Airport Operations Center immediately. The badge holder must remain at the door/gate and prevent access by others until Airport Operations personnel arrive and take control of the door/gate.
c. **Leaving an access point in "Time Override" unattended -** CLT SIDA badge holders who utilize "Time Override" or "Extended Hold-Open" features of access-controlled doors and gates are required to remain within sight of and maintain control over the door/gate to prevent unauthorized access. This section also includes circumstances when individuals misuse the time override or extended hold-open functionality. Badge holders are only permitted to utilize these functionalities to facilitate the boarding or deplaning of aircraft, or assist with deliveries where authorized. Any other use of these functionalities is not permitted, except with Airport Security Coordinator approval.
d. **Improper use of air crew code -** Use of an air crew PIN by CLT SIDA badge holders is prohibited.
e. **Piggybacking -** Following someone through an access point without the person using their own Badge or Key is prohibited.

#### 7.4.1 Securing Baggage Belts

The belts must be attended to at all times when they are running, or the security door on the belt is not secured. Only trained Badge holders are allowed to operate the baggage belts. The training must include procedures for transferring the responsibility for monitoring and security of the baggage belts between operators while the belts are in operation.

## 7.5 Challenge Responsibilities

### 7.5.1 Challenge requirement

Any Badge holder with unescorted access must challenge anyone who:

a. Is not displaying a SIDA Badge
b. Is acting suspiciously – looks out of place
c. Is attempting to piggyback or gain access to an area they are not authorized
d. Has challenged you. You must verify that they are also a valid Badge holder.

### 7.5.2 Challenge process

When challenging, ensure the following:

a. The Badge belongs to the person you are challenging and is still valid and is issued for CLT or is a CLT-approved Access Media. (Section 4.2)
b. The person has access to the area they are in or attempting to access. (Section 4.2).
c. The person has the appropriate endorsements for what they are doing; for example, ESCORT, DR (Section 4.2).
d. That you always "Respond to the Challenge" by asking for their Badge and following the same challenge procedure.

Violators will be subject to immediate removal from the Restricted Area and subject to notice of violation and potential TSA penalties.

**Note:** During a challenge process, you may ask to get a closer look at the Badge. Also, if an employee feels threatened / afraid to approach a person, they should immediately notify Airport Operations at 704.359.4012 (or 704.359.4911) and keep the person in sight and remain in the area until Security or Law Enforcement arrives unless it is physically unsafe to do so.

## 7.6 Responsibility for Reporting

All Badge holders must immediately report any observations of emergency situation, unauthorized persons in the restricted areas, or suspicious activity to Airport Operations at 704-359-4012, keep the person in sight, and remain in the area until Security or Law Enforcement arrives unless it is physically unsafe to do so. Suspicious activities or emergency situations include surveillance of the airport, including videotaping, photographing, and note-taking; persons exhibiting unusual behaviors; persons asking unusual questions or questions about airport security; persons or vehicles in the same location for an extended period; persons wearing improper clothing for their job or the weather; unattended bags, open, ajar, or unsecured doors to areas with restricted access, malfunctioning card readers, indicators of possible damage to the facility such as smoke, etc.

#### 7.6.1 Recording in Restricted Areas

Recording or releasing video or audio is prohibited in the following areas and situations, unless for a job-related purpose or approved in writing by the ASC.

a. Employee Inspections
b. Security procedures
c. Any other activities that would compromise the operational or security posture of CLT (including, but not limited to, medical emergencies, incidents, accidents, or active investigations).

## 7.7 Escorting

Any person with a CLT Badge with an "Escort" designation may escort under the following conditions (NOTE: The provisions below do not apply to vehicular escorting – please reference the CLT AOA Standards for these requirements):

a. The escort is for official business
b. Escorted person(s) not currently Badged **NOTE:** Individuals serving suspension, on leave, or whose badge has expired are considered Badged
c. Escorted person(s) must present a valid government-issued photo ID – Driver's License, Military ID, Passport
d. Badge holders with a Sterile Area Badge can be escorted into the Secured Area from the Sterile Area only for business purposes, such as to the Concessionaire's storage area or loading dock. **NOTE**: All Sterile Area Badge holders must first enter the Sterile Area through a TSA staffed screening checkpoint.
e. Escorted person(s) have not been previously denied a Badge for any reason
f. Escorted person(s) is/are accompanied, monitored & under control of the escort(s) at all times
g. Escorted person(s) only released to a Badge holder with escort privileges who has access to the area of escort
h. Escorted person(s) have been advised of their responsibilities when under escort
i. Escorted person(s) may only be engaged in activities they were escorted for (immediately removed if non-compliant)
j. Escorted person(s) and items are inspected for authorized Prohibited Items – (a written inventory of tools/Prohibited Items shall be available for inspection). Where the Escort fails to complete the inspection, and the escorted person introduces or attempts to introduce a Dangerous Weapon to the Restricted Area, the Escort's Badge will be Permanently Revoked.
k. The escort ratio must not exceed approved ratios, unless approved in writing by the

ASC. The approved escort ratios are available through the appropriate Authorized Signer.

l. Escorted persons who get separated must immediately stop; call the AOC at 704-359-4012, and advise the dispatcher of his/her name, location, and the name of his/her designated escort; and wait until his/her escort or a Law Enforcement Officer is able to locate him or her.

m. Escort who gets separated from their escorted person must contact the AOC at 704-359-4012 and continue to attempt to locate their escorted person.

**Note the following:**

1. Escorted person(s) and their items are the Escort's responsibility while under escort and can lead to notice of violation where such actions are in violation of these requirements.
2. Persons who have a continuous business need to access the Restricted Areas beyond 3 days in a 30-day period that have not submitted to the badging process may only be escorted with written approval from the ASC (ASC@cltairport.com).

# 8 Other Access Requirements

## 8.1 Personal Bag Restrictions

Employees working at CLT and individuals under escort are only authorized to use one personal bag and one lunch bag in the Secured/Sterile Areas of the Airport for the transport of personal items. Any personal bag will be subject to search at an access point or anywhere in the Sterile Area, Secured Area, or SIDA.

**Personal Bag**: Total dimensions cannot be more than 39 inches (H + W + D < 39”).

**Lunch Bag**: Total dimensions cannot be more than 32 inches (H + W + D < 32") and must be used only for food, drinks, utensils, and/or medicine. Only rounded-edge one-piece knives are allowed.

**Exceptions:**

a. Airline employees utilizing the Known Crewmember portal (not SIDA Badge holders)
b. Employees arriving on a flight and starting their shift (must have a boarding pass)
c. Airline Mechanics in uniform traveling on official business
d. One-time events approved by the ASC

**Note**: Employees flying after a work shift must keep travel bags outside of the Secured Area until the traveler is ready to process through screening for the flight. Any employee/contractor (and his or her items) utilizing a Badge to access the Secured or Sterile Areas is subject to

inspection by Airport, TSA, and Law Enforcement Officials. Individuals under escort when entering, or while in the Restricted Areas, are also subject to a search of their person and property.

## 8.2 Vehicle Access Procedures

### 8.2.1 Secured Area Access

When utilizing a vehicle to access the Secured Area, the following must be followed:

a. **Proper Identification and Authorized Driver Required**. All vehicles seeking to access the Secured Area or the AOA must be properly identified. Please reference the latest edition of the CLT AOA Standards for specific requirements related to vehicle signage and driver requirements.

b. **Badge Holder Responsibilities.** Badged vehicle drivers and passengers will be held responsible for complying with all security standards for their person and the vehicle in general, including, without limitations, compliance with the clear bag policy and Prohibited Item possession and use.

c. **Vehicles Subject to Inspection.** Vehicles seeking to access the Secured Area or the AOA may be subject to an inspection of the interior of the vehicle, including but not limited to the area under the seats, center console, and glove compartments; truck bed/cargo areas; and the undercarriage of the vehicle. Any large open containers, including large trash bags and trash cans found in the vehicle, will also be inspected. Vehicles may also be subject to search while in the Secured Area or the AOA. Once a vehicle attempts to access the Secured Area or the AOA, it is considered to be in the Secured Area or the AOA and subject to any relevant notice of violations and penalties up to and including Permanent Revocation of the Badge based upon the notice of violation issued. **NOTE:** The vehicle operator is required to wait for inspection at any staffed vehicle gates. Failure to wait will result in a security violation.

d. **Screening of Vehicle Operators and Passengers**. The driver and all occupants attempting to access the Secured Area or the AOA are subject to screening and must have valid identification in their possession.

e. **Tailgating.** Driving a vehicle through a vehicular gate behind another vehicle without the driver using their own Badge to authorize access is prohibited.

f. **All individuals requesting access must** cooperate with law enforcement, CLT staff, TSA, or other individuals charged with implementing the provisions of the ASP, or other rules and regulations of CLT.

### 8.2.2 Access through Security Gate

If a vehicle operator is attempting to access the Secured Area or the AOA through an access-controlled gate, the driver and each badged occupant in the vehicle must swipe his/her Badge at the access reader.

a. If the Badge reader displays a green light and the Badge holder has driving privileges, the gate will open.
b. If the Badge holder does not have driving privileges on their Badge, but they do have access to the gate, the reader will display a green light, but the gate will not open.
c. If the Badge reader displays a red light for any occupant's CLT Badge, the attendant will deny access and confiscate the Badge.

### 8.2.3 Denial of Access

CLT reserves the right to deny access to any vehicle operator attempting to access the restricted areas of CLT in circumstances where:

a) The vehicle, operator, and/or contents of the vehicle are non-compliant with Federal Regulations governing vehicle access and operations on the AOA.
b) A vehicle is deemed unsafe for use on the AOA (Reference the CLT AOA Standards for more information on vehicle readiness).
c) It is determined that the vehicle operator does not have an operational need to access the restricted areas of CLT.
d) Vehicle operators are non-compliant with required processes listed above.

## 8.3 Vehicle Escort Procedures

Vehicle Escorting shall be for business purposes only. The following procedures and requirements should be followed:

a. Motor Vehicles that provide an escort into the Secured Area or the AOA must be authorized to operate in that Area;
b. CLT has a Non-Movement Driver's licensing program. The Non-Movement course is required for ALL individuals operating any motorized vehicle in the Secured Area or the AOA not under vehicular escort. Successful completion of the Non-Movement Driver program will result in the "DR" designation on the CLT Badge. No individual may operate a motorized vehicle on the AOA without the "DR" designation on their Badge. Any driver without a "DR" endorsed CLT Badge must be under the escort of an approved CLT vehicle or a badge holder with the vehicular escort “DR-E” endorsement on their badge. Having a "DR" only endorsed CLT Badge does not authorize the Badge holder to conduct a vehicular escort of another vehicle in the Secured Area or the AOA.

c. The driver of the vehicle that is under escort must provide the guard with his/her driver's license and vehicle information.
d. All vehicles must adhere to the Vehicle Contact Card requirements in the CLT AOA Standards.
e. Drivers of motor vehicles being escorted must stay with their motor vehicle until it leaves the Secured Area or the AOA.
f. The escorted vehicle must follow and stay with the vehicle providing escort at all times while under escort.
g. Prior to escorting a vehicle into the Secured Area or the AOA, an escort shall inform his/her escortee of all requirements to properly be within the Secured Area or the AOA, perform an inspection, and notify them of the procedures to follow if they get separated during the escort.
h. Escortees, should they get separated, must immediately stop the vehicle; call Airport Operations at 704-359-4012 and advise the dispatcher of his/her name, location, and the name of his/her designated escort; and wait until his/her escort or a law enforcement officer is able to locate him or her.

## 8.4 CLT Computer Systems Access Requirements

Any computer systems that CLT provides to staff and tenants for use, including CLT's Video Management System ("VMS"), Authorized Signer Portal ("AS Portal") for processing Credentialing applications, ID Management System (IDMS), Access Control System, or others, are classified as containing Sensitive Security Information ("SSI"), or Personally Identifiable Information ("PII"). Users of these systems must have an active badge and are granted access subject to compliance with the following:

a. Users are required to complete training before being granted access and repeat it annually to maintain access.
b. The user can only access these systems to complete official work responsibilities.
c. The user is responsible for notifying the ASC or designee if any unauthorized use of these systems is observed or reported.
d. The user must comply with all directives governing the use of these systems.
e. The user is prohibited from allowing, whether intentionally or unintentionally, any person to use or access his or her login credentials. Notwithstanding this express prohibition, the user is authorized to use these systems with team members who do not possess access to the VMS for official purposes only and is responsible for all actions performed during the use of his or her login credentials. **NOTE:** Sharing login information will result in permanent revocation of the user's badge.
f. The user must log off when not using these systems to avoid unauthorized use;

g. The user must not share his or her password. Passwords will expire after 90 days and must be changed. If the account is inactive for periods of 30 days or more, the account will be disabled.
h. The user is prohibited from downloading, recording, and/or releasing any video footage, PII, badge information or any other system-generated information, without written permission from the ASC or designee, to any entity, including, but not limited to, other law enforcement agencies (local, state, or federal), the State Attorney's Office, the United States Attorney's Office or any news organization. **NOTE:** Unauthorized release of video footage, PII, badge information, and/or any other system-generated information will result in permanent revocation of the user's badge.
i. The user is prohibited from recording video of any footage from the VMS with any cell phone, video camera, data device, or any other device capable of recording video. Notwithstanding the express prohibition, a still photo may be taken and distributed by law enforcement personnel and TSA employees, but only for law enforcement or TSA investigation purposes and only if absolutely necessary.
j. The user shall abide by all policies, requirements, and guidelines instituted by CLT.

CLT monitors and audits these systems to ensure proper usage of the system and reserves the right to limit or remove access at any time. Failure to comply with these requirements or any other directive issued by CLT can result in a Security Violation notice of violation, up to and including permanent Badge revocation, revocation of access to these systems, and federal penalties.

Any Airport Users who wish to install their own CCTV systems, which are independent of the CLT's system, may do so only with the approval of CLT and must enter into a Memorandum of Understanding (MOU) with CLT. Failure to enter into the MOU will result in a denial of such a CCTV system. Airport Users who may currently have their own CCTV system must enter into the MOU by 31 December 2023.

## 8.5 Compliance Testing

Security compliance testing may be performed only by those individuals authorized by 49 CFR 1540.105(b), the Airport Security Program, and those specifically authorized by the primary Airport Security Coordinator. The ASC or designee may conduct compliance testing without written authorization. CLT SIDA badge holders are required to comply with authorized compliance testing.

## 8.6 Clear Zone

CLT maintains a clear zone of 6 feet on either side of the SIDA fence (10 feet on either side of the fence when the SIDA fence is less than 10 feet in height). Vehicles, structures, or any

implement/item/tool that would allow access through, under, or over the SIDA fence must not be stored or left unattended in the clear zone.

# 9 Security Violations and Related Penalties

## 9.1 General Information

When an Airport User, AS, or Badge holder fails to comply with the responsibilities or obligations set forth in these Security Standards or in the ASP, they will be held accountable. The severity of the accountability and resulting consequences depends upon the specific act of non-compliance. The various types of notice of violations, violations, and possible consequences are as follows:

## 9.2 Tier 3 Violations – Permanent Revocation

**All Tier 3 infractions will result in immediate suspension and confiscation of SIDA credentials and penalties that may include permanent revocation of the Badge.** Badge holders will be escorted to the non-sterile or public area and receive a notice of violation pending a scheduled hearing.

| Section | Description | Tier |
|---|---|---|
| 4.2.1 | Who must be screened | 3 |
| 5.4.1 | Sharing authorized signer portal login | 3 |
| 5.4.1e | Authorized signer acknowledging the disqualifying crimes statement for another. | 3 |
| 5.4.2 | Access media application violation (falsification/fraud) | 3 |
| 6.2.7b | Inappropriate conduct on airport premises | 3 |
| 6.2.7c | Conviction of a misdemeanor or felony committed on airport property | 3 |
| 6.2.7d | Disqualifying crime violation | 3 |
| 7.2b | Use/allowing use of another's access media | 3 |
| 7.2e | By-passing TSA and/or CLT security/screening/inspection measures | 3 |
| 7.2g | Failure to comply with screening/searches (person) | 3 |
| 7.2h | Copying, reproduction of access media | 3 |
| 7.2i | Using a key to bypass a door equipped with a card reader | 3 |
| 7.3.2 | Dangerous weapon, incendiary, ammunition violation | 3 |
| 8.2.1c | Failure to comply with screening/inspection (vehicle) | 3 |
| 8.4g | Sharing login for CLT security computer systems | 3 |
| 8.4h | Unauthorized release of video footage | 3 |
| | Actions resulting in fines to the City of Charlotte for violations by a federal or regulatory entity | 3 |

**Note:** All violations, except for Inappropriate Conduct. would also result in an entry into the Centralized Revocation Database ("CRD") that is maintained by the DHS.

## 9.3 Permanent Badge Revocation Hearing and Appeals (Tier 3)

For severe violations (Tier 3), where a person's Badge is or can be immediately and/or permanently revoked, the employee will be offered a scheduled revocation hearing arranged by the ASC or their designee. At this meeting, all the information and facts related to the violation will be reviewed and evaluated to ensure the penalties assessed are appropriate for the severity of the violation. Every effort will be made to complete this process as soon as possible, but it may take up to 30 days. NOTE: Violators who do not attend the hearing without good cause will not be eligible for an appeal.

The review panel will consist of Alternate Airport Security Coordinators. Any appeals will be submitted to the ASC. Information detailing the appeal process will be provided to the violator and their employer. The violator's name will also be entered into the CRD that is maintained by the DHS. Employee and employer fines must be paid within 30 calendar days. Failure to do so will result in an interruption of new badge requests and renewals until paid in full.

## 9.4 Infractions (Tier 1 and 2 violations)

| Section | Description | Tier |
|---|---|---|
| 4.1.2 | Visitor pass program violation | 1 |
| 6.1.2c | Unauthorized modification to tenant lease areas that impact security | 1 |
| 6.1.2d | Unauthorized events held in restricted areas | 1 |
| 6.1.2f | Deliveries of merchandise or consumables to the restricted areas violation | 1 |
| 6.2.2 | Failure to immediately report lost, destroyed, or stolen SIDA badge (employee/badge holder) | 1 |
| 6.2.7a | Other violations of CLT Security Standards | 1 |
| 6.3.2 | Unauthorized use of SIDA badge for construction project (contractor/sub-contractor) | 1 |
| 6.4.1 | Improper access to Sterile Area (concessionaires) | 1 |
| 7.1 | Failure/Improper display of SIDA badge | 1 |
| 7.2a | Improper use of access media (general) | 1 |
| 7.2f | SIDA badge use/display for wrong company | 1 |
| 7.3.1 a | Missing inventory of tools of the trade | 1 |
| 7.6 | Failure to report emergency/suspicious activity | 1 |
| 8.1 | Personal Bag violation | 1 |
| 8.2.1a | Vehicle signage violation | 1 |
| 8.4 | CLT computer system violation (general) | 1 |
| **Section** | **Description** | **Tier** |
| 8.6 | Clear zone violation | 1 |

| | Violations of the Airport Security Program or 49 CFR 1540/1542 not included in the CLT Security Standards | |
|---|---|---|
| 3 | Failure to comply with the requests of staff enforcing the ASP | 2 |
| 5.4 | Authorized signer violation | 2 |
| 5.6.4 | Failure to notify Credentialing of a disqualifying crime conviction/finding | 2 |
| 5.6.6 | Unauthorized dissemination of CHRC results | 2 |
| 5.6.9 | Failure to maintain the confidentiality of credentialing records | 2 |
| 6.1.2a | Failure to secure the security doors located in the tenant lease area | 2 |
| 6.1.2e | Concessionaire prohibited item and knife audit violation | 2 |
| 6.2.c | Failure to deactivate the SIDA badge (authorized signer) | 2 |
| 6.2.5 | Failure to return the SIDA badge (employee or employer) | 2 |
| 6.2.8 | Failure to comply with CLT audit (Credentialing) | 2 |
| 6.3.1 | Failure to obtain a sponsorship letter (contractor) | 2 |
| 6.3.3 | Failure to properly secure the construction/laydown area | 2 |
| 6.4.2 | Knife and Prohibited Item violations (concessionaires) | 2 |
| 7.2c | Expired SIDA badge (use/display/possess) | 2 |
| 7.2d | Use of access media for non-business purposes/hours | 2 |
| 7.3 | Prohibited item violation | 2 |
| 7.3.1 b-f | Prohibited Items Necessary for the Performance of Job Duties | 2 |
| 7.4 | Access Point Violation | 2 |
| 7.4.1 | Baggage belt violation | 2 |
| 7.4 a | Leaving an access point unattended | 2 |
| 7.4 b | Leaving an access point in "Time Override" unattended | 2 |
| 7.4 c | Improper use of the air crew PIN | 2 |
| 7.4 d | Piggybacking | 2 |
| 7.5 | SIDA badge challenge violation | 2 |
| 7.7 | Escort violation (person) | 2 |
| 8.2.2 | Failure to follow proper procedures when entering an access-controlled gate | 2 |
| 8.3 | Escort violation (vehicle) | 2 |
| 8.4e | Permitting authorized access to CLT security computer systems | 2 |
| 8.4f | Failure to log off CLT security computer systems | 2 |
| 8.4i | Unauthorized recording of video footage from CLT security systems. | 2 |
| 8.5 | Failure to comply with compliance testing | 2 |

A combination of any **three** or more Infractions within a rolling thirty-six (36) month period will result in **permanent revocation of the person's Badge.**

## 9.5 Issuance of Notice of Violation (Tier 1 and 2 violations)

Once a violation of the security program has occurred, a notice of violation can be issued in several ways:

a. By email
b. In person - Your access media temporarily suspended until you are located
c. Delivered to your supervisor/manager.

## 9.6 Appealing a Notice of Violation (Tier 1 and 2 violations)

After receipt of the notice of violation, the violator has an opportunity to appeal. The appeal process for the Badge holders is in the email with the issuance of the security violation. The violator has three business days to appeal in writing to the Notice of violation Review Board ("NVRB"). All appeals must be submitted by email listed in the notice of violation notification. Appeals submitted after the three business day deadline will not be taken into consideration.

In most cases, employees will be able to continue to use their Badge while the adjudication process moves forward, with the exception of severe violations (Tier 3).

The NVRB will hear evidence and issue a finding that supports CLT's Airport Security Program: Dismissed, Warning, Penalties. An electronic letter will be sent to the violator and their employer with the NVRB disposition of the violation. The violator must coordinate with his or her employer to satisfy the requirements of the NVRB's findings and penalties as applicable. The appeal process will typically take from seven to 30 days.

## 9.7 Appeal Review (Tier 1 and Tier 2 violations)

Upon notification of the decision of the NVRB, the violator has 30 days to appeal the decision in writing to the ASC. The email address for this appeal will be provided in the letter with the decision of the NVRB. Individuals who miss the scheduled hearing are not eligible for an appeal of the NVRB decision, unless they have notified the NVRB of their inability to attend in advance.

## 9.8 Progressive Discipline and Fine Schedule

Failure to comply with the above CLT Security Standards will result in immediate disciplinary action per the following disciplinary schedule. As described in this document, the ASC has the discretion to escalate or de-escalate the penalty tier if unique circumstances exist to justify such a modification. All infractions will be documented, tracked, and will remain on the individual's record for thirty-six (36) months. Additionally, any violations of the CLT Security Standards

determined to be egregious in nature by the ASC may be subject to additional monetary fines and/or elevated disciplinary actions. The discipline schedule is as follows:

| CLT | Tier 1 | Tier 2 |
|---|---|---|
| First Offense | Written or verbal Warning and education on the spot | Badge Confiscation/up to three days - SIDA re-training and monetary fines per the current fine schedule |
| Second Offense – any offence within the last 36 months | Badge Confiscation/up to three days - SIDA re-training and monetary fines per the current fine schedule | Badge Confiscation/up to seven days. SIDA re-training with the manager/supervisor, and monetary fines per the current fine schedule |
| Third Offense - any offense within the last 36 months | Badge Confiscation/up to seven days.<br>SIDA re-training with the manager/supervisor, and monetary fines per the current fine schedule | Permanent Revocation of SIDA badge and entry into the CRD that is maintained by the DHS. Will be treated procedurally as a Tier 3 infraction. |
| | | |
| **Tier 3**<br>**All Tier 3 infractions will result in immediate suspension of SIDA credentials & penalties that may include:** | | |
| First Offense | ▪ Permanent revocation of badge | |
| *For Tier 3 violations, the review panel will consist of Alternate Airport Security Coordinators. Any appeals will be submitted to the ASC. Information detailing the appeal process will be provided to the violator and their employer. The violator's name will also be entered into the CRD that is maintained by the DHS. Employee and employer fines must be paid within 30 calendar days. Failure to do so will result in an interruption of new badge requests and renewals until paid in full.* | | |

The violator and authorized signer must make arrangements to satisfy the fines, suspension, training, or other requirements with the Credentialing office (AVBadging@cltairport.com) within 14 business days of being notified. Failure to make arrangements or satisfy the required penalties will result is suspension of the violator's access privileges at CLT.

**Note:** If an individual is employed by multiple companies and has multiple badges, all active badges will be suspended. Additionally, badges for new employment will not be activated until the violation has been completely resolved.

## 9.9 Additional Monetary Fines

The fines described herein are a general guideline for fines. The NVRB or ASC may increase or decrease the amount of the fine based on the circumstances of the violation. The following is are tiered badge reactivation fee schedule:

| | |
|---|---|
| First Offense | $100.00 |
| Second Offense | $200.00 |
| Third Offense | $300.00 |

**Note:** All penalties and fines listed in sections 9.8 and 9.9 are separate from any actions taken by the employer or the TSA. Additionally, all fines assessed must be paid in full by the person or entity that committed the violation. Separate entities or persons cannot be billed for fines assessed for security violations.

## 9.10 Conduct Violations

Any instances of inappropriate conduct listed in section 6.2.7 at CLT will result in a conduct hearing for the employee committing the violation and their employer with the ASC group. The ASC group will determine the penalties up to and including permanent revocation of the badge.

## 9.11 Employer Responsibilities

It is the employer's responsibility to ensure that its employees understand and obey the rules and regulations contained within these standards. The following steps should be taken to ensure a secure environment at CLT:

**Training:** Employers should conduct appropriate training to ensure that all personnel have read and fully understand the guidelines set forth within these standards.

**Monitoring:** Employers should monitor their personnel and ensure that they have knowledge of the regulations and are adhering to the rules set forth within these standards.

**Follow-Up:** Employers will be notified of any notice of violations issued to their employees. Therefore, employers should follow up on all notices of violations issued to their employees and ensure that appropriate action is taken to prevent further incidents.

Nothing in these standards shall be construed or interpreted as creating or establishing the relationship of employee and employer between the City of Charlotte and any tenants, vendors, contractors, subcontractors, or any individuals working for said entities.

## 9.12 Airport User Fines and Penalties

Airport Users can be penalized for security violations as a company, as well as holding Badge holders or the company AS accountable individually (for a single violation, the company and the individual may be cited). Examples include: encouraging employees to commit violations, negligent actions, not being responsible in reference to security, or not supporting and/or enforcing the Security Program, and/or assessed notice of violation penalties, or continuous and/or habitual violations by Airport User employees.

Fines or monetary penalties assessed against CLT by the TSA or other regulatory agency, after all appeals have been exhausted, for infractions or violations of applicable TSA regulations, may be passed on to the airline/tenant involved or equally assessed between the airline/tenant and CLT. CLT has the sole responsibility, in its discretion, to contest or not contest fines.

All tenants agree to cooperate fully with CLT in any investigation into a possible security violation.

Airport Users may appeal any notice of violation following the appeal process set forth in Section 9.6

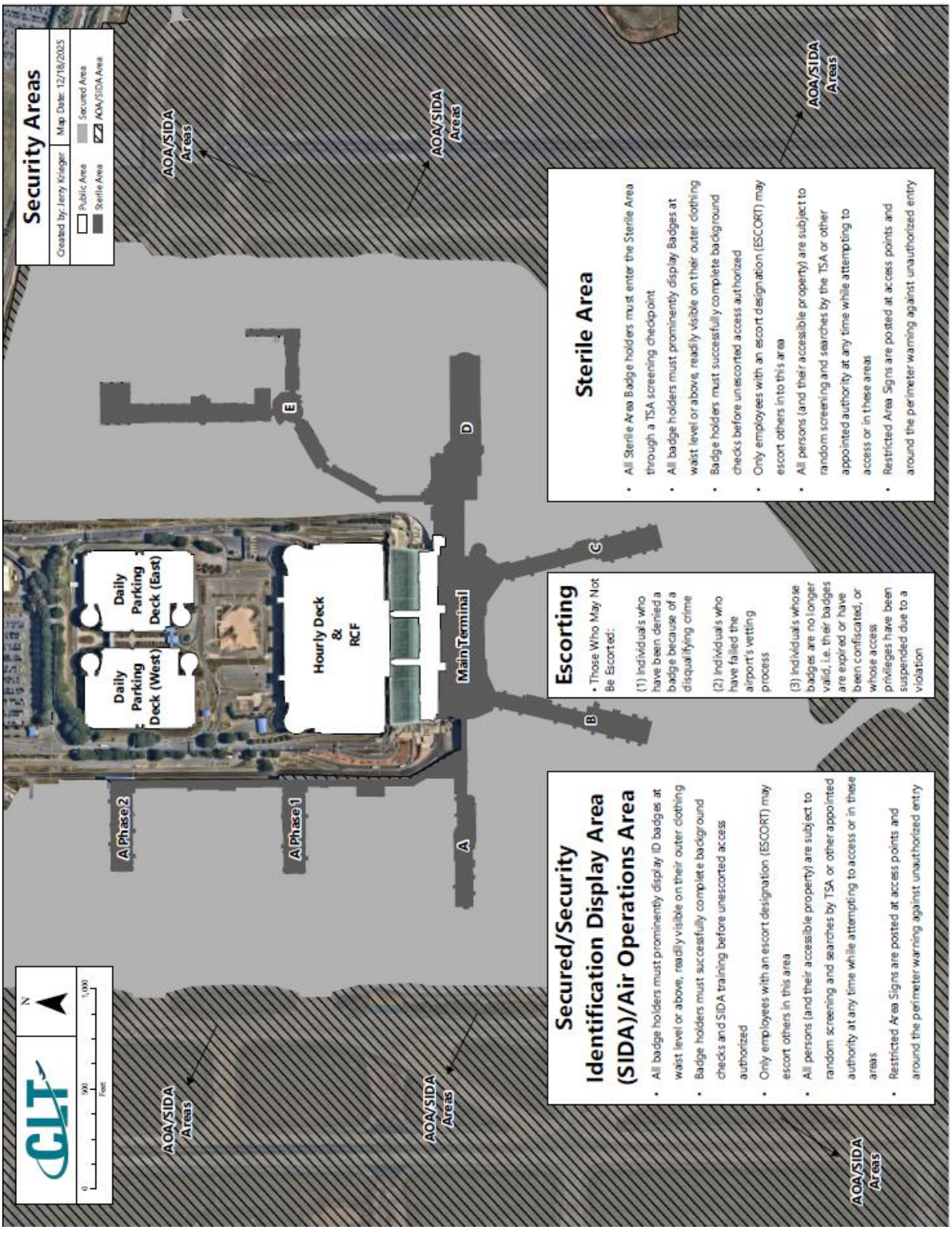
Any tenant that is found non-compliant with the Employer Responsibilities described in these Security Standards shall be assessed the following fines:

| | |
|---|---|
| First Offense | Written Warning issued to the employer |
| Second Offense | $500 fine assessed against the Airport User |
| Third Offense | $1,000 fine assessed against the Airport User |
| Fourth Offense | $2,000 fine assessed against the Airport User |
| Fifth Offense | Event of default |

At the ASC's discretion, chronic and/or blatant violations of security procedures may result in fines of up to $10,000, depending on the severity and circumstances of the violation(s). Appeals by Company, Tenant, or Contractor fines can be submitted in writing to the ASC for consideration.

# Appendices

# Appendix 1


Security Areas
Created by Jerry Krieger
Map Date: 12/18/2025
Public Area
Sterile Area
Secured Area
AOA/SIDA Area
AOA/SIDA Areas
Daily Parking Deck (East)
Daily Parking Deck (West)
Hourly Deck & RCF
Main Terminal
A Phase 2
A Phase 1
A
B
C
D
E
Sterile Area
All Sterile Area Badge holders must enter the Sterile Area through a TSA screening checkpoint
All badge holders must prominently display Badges at waist level or above, readily visible on their outer clothing
Badge holders must successfully complete background checks before unescorted access authorized
Only employees with an escort designation (ESCORT) may escort others into this area
All persons (and their accessible property) are subject to random screening and searches by the TSA or other appointed authority at any time while attempting to access or in these areas
Restricted Area Signs are posted at access points and around the perimeter warning against unauthorized entry
Escorting
Those Who May Not Be Escorted:
(1) Individuals who have been denied a badge because of a disqualifying crime
(2) Individuals who have failed the airport's vetting process
(3) Individuals whose badges are no longer valid, i.e. their badges are expired or have been confiscated, or whose access privileges have been suspended due to a violation
Secured/Security Identification Display Area (SIDA)/Air Operations Area
All badge holders must prominently display ID badges at waist level or above, readily visible on their outer clothing
Badge holders must successfully complete background checks and SIDA training before unescorted access authorized
Only employees with an escort designation (ESCORT) may escort others in this area
All persons (and their accessible property) are subject to random screening and searches by TSA or other appointed authority at any time while attempting to access or in these areas
Restricted Area Signs are posted at access points and around the perimeter warning against unauthorized entry
N
0
500
1,000
Feet

# Appendix 2

**Disqualifying Crimes**

(1) Forgery of certificates, false marking of aircraft, and other aircraft registration violations, 49 U.S.C. 46306.
(2) Interference with air navigation, 49 U.S.C. 46308.
(3) Improper transportation of hazardous material, 49 U.S.C. 46312.
(4) Aircraft piracy, 49 U.S.C. 46502.
(5) Interference with flight crewmembers or flight attendants, 49 U.S.C. 46504.
(6) Commission of certain crimes aboard aircraft in flight, 49 U.S.C. 46506.
(7) Carrying a weapon or explosive aboard aircraft, 49 U.S C. 46505.
(8) Conveying false information and threats, 49 U.S.C. 46507.
(9) Aircraft piracy outside the special aircraft jurisdiction of the United States, 49 U.S.C. 46502(b).
(10) Lighting violations involving transporting controlled substances, 49 U.S.C .46315.
(11) 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.
(12) Destruction of an aircraft or aircraft facility, 18 U.S.C. 32.
(13) Murder.
(14) Assault with intent to murder.
(15) Espionage.
(16) Sedition.
(17) Kidnapping or hostage-taking.
(18) Treason.
(19) Rape or aggravated sexual abuse.
(20) Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon.
(21) Extortion.
(22) Armed or felony armed robbery.
(23) Distribution of, or intent to distribute, a controlled substance.
(24) Felony arson.
(25) Felony involving a threat.
(26) Felony involving:
- (i) Willful destruction of property
- (ii) Importation or manufacture of a controlled substance;
- (iii) Burglary
- (iv) Theft
- (v) Dishonesty, fraud, or misrepresentation
- (vi) Possession or distribution of stolen property
- (vii) Aggravated assault
- (viii) Bribery, or
- (ix) Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than 1 year.

(27) Violence at international airports 18 U.S.C. 37.
(28) Conspiracy or attempt to commit any of the criminal acts listed in this paragraph (d).

# Appendix 3

## Charlotte Douglas International Airport
### Security Identification Badge Rules and Regulations

**APPLICANT MUST RETAIN THESE RULES AND REGULATIONS**

**Notice:** More information on the below rules and regulations, as well as possible penalties for not following them, is described in the *CLT Security Standards* and *CLT AOA Standards* that can be accessed at www.cltairport.com/business/credentialing. The Authorized Signer should also be able to provide you with a copy. All Badging Rules and Regulations are under continuous review and subject to revision. All Badge Holders agree to comply at all times with CLT Security Standards and other rules and regulations, including provisions of Title 49, CFR, Parts 1540, 1542, and 1544 as applicable.

- The following Security Violations will likely **result in immediate and permanent revocation** of a CLT SIDA badge and entry into the Centralized Revocation Database ("CRD") that is maintained by the DHS; **Initial:** _____

  - *Loaning/Borrowing an ID Badge to/from Another Person (Revocation of both person's Badges).*
  - *Loaning/Borrowing Security Keys to/from Another Person (Revocation of both person's Badges).*
  - *Falsification, copying, reproduction of CLT Access Media, application, or documentation for Credentialing purposes, and any other fraud.*
  - *Bringing in or possessing dangerous weapons, explosives, and/or ammunition on Airport property*
  - *Bypassing Screening - Employee access and Passenger screening*
  - *Sharing AS Portal login information.*
  - *Responding to the disqualifying crimes questions for the applicant.*
  - *Sharing login information for CCTV systems.*
  - *Unauthorized release of video surveillance footage.*

- **Multiple Badge holders -** In addition to the provisions in the Security Training Program and CLT Security Standards, employees that have been issued more than one (multiple) badges at CLT Airport accept security responsibility as a multi-badge holder, which includes;

  - Use of each badge issued and the access authority assigned to it, only for the purpose for which the employer that authorized it had intended.
  - Accept that use of a badge to gain access to an area that is not authorized to me during the times that I am not performing duties that are assigned that access can result in suspension or revocation of all access authority for all badges issued to me.
  - Accept that CLT and/or the Transportation Security Administration (TSA) may levy fines, sanctions, or penalties against me for misuse.

**Signature** _____ **Date:** _____

- Employees can only be badged by their employer(s) CLT security identification **badge is for official use only** and is NOT to be used for personal or off-duty/work purposes

- Keys are only issued to individuals that possess valid CLT security identification badges.

- CLT security identification **badges, access keys, and parking placards are the property of CLT** and must be surrendered upon request and/or within 48-hours when it is no longer required for the performance of my duties, termination of employment, or work assignment at CLT

- **Failure to immediately deactivate** CLT security identification badges or access keys when access is no longer required will result in a fine.

- **Application -** 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) every two years or enroll the individual in a continuous vetting program (Rap Back).

- 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. Original, unexpired identification and work authorization documents will be presented at the time applications and fingerprints are completed.

- 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.

- 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.

- Individuals applying for unescorted access to the Secured or Sterile areas of the airport must successfully complete the required security training.

- Badge holders and authorized signers have a continuing obligation under 49 CFR 1542.209(l) to **disclose to CLT within 24-hours if a badge holder is arrested or convicted of any disqualifying criminal offense** that occurs while they have unescorted access authority.

- Applicants must obtain their CLT security identification badge within 30-days of notification that the applicant's background has been completed. If the badge is not received within the 30-days, a new application will need to be submitted.

- All persons in the SIDA, Secured and Sterile Areas, and Air Operations Area (AOA) will be required to display on their persons, at all times, the properly issued CLT security identification badge. The CLT security identification badge will be displayed above the waist on the outer garment so as to be clearly visible.

- It is the responsibility of each CLT security identification badge holder to challenge any individual not displaying their CLT security identification badge while on Airport property, and each CLT security identification badge holder is required to produce their CLT security identification badge when challenged or upon request by TSA, law enforcement, Airport staff or employer.

  *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 a CLT security identification badge, the individual conducting the challenge must remain with the un-badged person and immediately report this incident to CLT Airport Operations 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 CLT Airport Operations to report the incident.*
  - *The 24-hour CLT Airport Operations Center emergency notification number is 704-359-4012, located on the back of the CLT security identification badge.*

- Each person must enter AOA and SIDA/Secured Area using their issued CLT security identification badge unless under escort Multiple persons entering an automated access point on a single entry transaction is PROHIBITED. The only exceptions are doors without card readers and aircrews using doors with PIN-only access. All badge holders shall wait until the door or gate is fully closed before leaving the area.

- **If an alarm is activated**, the individual must remain in the area and immediately contact CLT Airport Operations and provide a resolution to the alarm.

- **Escorts** must comply with the following conditions:
  - *Escorting is allowed for a business purpose only*
  - *Only authorized individuals with proper endorsement on their badge are allowed to escort*
  - *Only unbadged individuals may be escorted*
  - *Escorts must continually maintain visual and audible contact at all times with those under escort while in regulated areas, 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 CLT Airport Operations Center for assistance.*
- All lost, misplaced, or stolen CLT security identification badges or keys must be immediately reported to the CLT Credentialing office at 704-359-4010 during normal business hours or to Airport Operations 704-359-4012 after business hours. Badge fee may be assessed.

- 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 their initial badge and each time they renew their badge. Applicant/badge holder must present a valid driver's license for verification. If a badge holder's driver's license is suspended or expired, the DR endorsement will be removed.

- CLT security 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 for ensuring persons utilizing these gates are in compliance with CLT and TSA Regulations, including verification of name(s) against the Stop List. Gate monitors must have a current Stop List in their possession at all times.

- All CLT security identification badge holders must renew their security badge before the expiration date, which is listed on the front of the badge. The process of renewal may begin up to 30-days prior to the expiration. CLT badge application must be completed each time the badge is renewed.

- CLT badge holders who do not renew expired badges 30-days after expiration will need to complete a new badge application and undergo a new STA before a badge is issued. Use of an expired badge is a security violation and may result in denial of badge renewal, criminal and/or civil penalties.

- CLT reserves the right to refuse or revoke authorization of any individual for CLT security identification badges where such action is determined to be in the best interest of airport security for reasons including, but not limited to inappropriate conduct at CLT, arrests for crimes committed on airport property, causing damage to CLT property.

- **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. Individuals accessing or present within the Sterile Area, Secured Area, SIDA, AOA, or boarding aircraft are subject to search of their person and accessible property. Aviation workers possessing airport-issued identification (ID) media and their Escorts are subject to screening for unauthorized weapons, explosives, and incendiaries. Non-compliance with the airport operator's aviation worker screening policy could result in penalties, which may include confiscation of their airport operator¬ issued ID media and/or revocation of unescorted access authority.

- No information may be released that may compromise the contents of CLT's Airport Security Program, including posting and sharing of such information on social or other media forums.

- Badge holders must comply with the clear bag policy. All employees working at CLT are only authorized to use one Clear Bag and one lunch bag in the Secured/Sterile Areas of the Airport for transport of personal items. Any personal bag will be subject to search at an access point or anywhere in the Sterile Area, Secured Area, or SIDA.

- Employees should **review the contents of the *CLT Security Standards*** for a complete and comprehensive list of security requirements. Failure to comply with the rules and regulations may result in temporary or permanent revocation of access and/or pay monetary fines.

**Signature** _____ **Date:** _____