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

1 749′ MSL

I. Revision Checklist

Revision List	
Issued 04/2020 (New edition)	

Contents

II. Appendices	
Appendix 1	Security Areas
Appendix 2	Disqualifying Crimes
Appendix 3	Security Identification Badge Rules and Regulations
Appendix 4	Examples of Disallowed Clear Bags

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 direction 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 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 assuring 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 to 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 adjucation 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.

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

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

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 – Web site that allows AS secure access to manage the Badge holders for the Airport User.

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

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 activies.

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 the 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.

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 - As defined by Section 15-14 of the Charlotte City Ordinance is any object or device designed or intended to be used to inflict serious injury upon persons or property, including, but not limited to, firearms, including ammunition; knives of any kind or type having a blade in excess of 3½ inches in length, except when used solely for preparation of food, instruction or maintenance; razors and razor blades, except when used solely for personal shaving; metallic knuckles; clubs, blackjacks and nightsticks; dynamite cartridges, bombs, grenades, mines and other powerful explosives; slingshots; shurikens; stun guns; and loaded canes; or any other items that are or will be prohibited by the City, the TSA, the FAA, or any other regulatory body.

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

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.

ESCORT (designation on Badge) – Individuals authorized to accompany or escort unbadged individuals in the restricted areas.

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 designated Authorized Signer has submitted a complete and accurate application.

LEO – Law Enforcement Officer.

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

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 tsa.gov website. This term does not include Dangerous Weapon.

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

Restricted Areas – Areas not open to 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.

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 support services for the operation of airport tenants (those with leaseholds) and do not 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, Airport Tenants or Concessionaires.

3 Compliance Requirements

All users of CLT must comply with these Security Standards, as well as applicable laws, regulations, directives and policies, 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 responsibilies of Access Media holders, and the citations 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

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;
d. Persons having prior written CLT authorization; and
e. Properly identified FAA or DHS employees or representatives.

4.2 Security Screening

Who Must be Screened. 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 review of items on your person, in your personal belongings, and of your Badge. If an invalid Badge is presented, Prohibited Items 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 Airport Operations at 704-359-4012 and both individuals reporting the incident and those in violation must stay onsite 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.

CLT Issued Badge Description and Authorization. CLT issues Badges which 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
	RED Sterile Area Only	Must gain access the Sterile Area through a TSA screening checkpoint only
	Green - CLT Secured/Cargo Areas	Secured Area, the AOA west of runway 18L/36R, and the Sterile Areas
	Orange - CLT GA/South Cargo Areas	AOA south of taxiway C8, the FBO east of runway 18L/36R, and Sterile Areas
	Gray - CLT Public Areas	Areas prior to security checkpoints only. Issued to taxicab drivers, curbside valet personnel.
	Blue - CLT All Areas	All areas of CLT
Endorsements by Badge: ESCORT – Escort Privileges; DR – AOA Driving privileges; Customs Seal – Access to Federal Inspection Station area; **Command Post -** authorization to enter the ICC or emergency scene		

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 are 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 Use of Form 110A. While Form 110A is considered an official identification medium while 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

Credentialing provides the following services **with appointments**;

a. Badge related regulatory Training
b. Fingerprinting for applicants

c. New Badge Issuance
d. Badge Renewals
e. Badge changes; endorsements, including Customs Seal additions.

Credentialing provides the following services **without appointments**;

a. Badge returns and Badge status changes
b. Solicitation Permits
c. Restricted Area and Parking Access Changes. (w/written documentation)

5.2 Determination of Eligibility for Issuance of a CLT Badge

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 finger print check. Their governmental agency identification badges will be accepted as verification that a prior employment check has been completed.

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.

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: (i) authorize a direct employee or a sponsored company employee to proceed with the fingerprint process conducted by CLT or the Air Carriers; and (ii) 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.

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

Background Checks. To determine badging eligibility, TSA requires all applicants to pass both the CHRC and STA. Air Carriers (1544 companies) are permitted to conduct the CHRC independently, but are required to provide certification that the applicant has not been convicted of disqualifying criminal offense. Such certification shall include the Offense Cycle Number (OCN) and date of fingerprinting and CHRC results. Air Carriers will be held responsible for ensuring these checks are completed in accordance with federal regulations. The ASC may not require the Aircraft Operator to provide a copy of the criminal history record check completed by the Aircraft Operator.

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 limits the number of AS designations up to four (4) per Airport Tenant or Air Carrier with less than 500 employees. Exceptions are made for those with over 500 employees on a case by case basis. An updated authorized signer letter which includes the names of those authorized to sign must be kept on file with Credentialing. 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

5.4 Authorized Signer Badge Application Responsibilities.

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 Badge applications and initiate a 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 that will result in ***permanent Badge revocation*** 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, SSN.
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 applicants email on file. **NOTE:** This acknowledgement cannot be done by the AS. It is considered a falsification of records if the AS completes this for the applicant and 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. Scheduling 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. AS are required to comply with Security Standards that govern the credentialing process. AS are also responsible for safeguarding their portal login information, returning Keys, Security Keys and Badges, 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 Section 9.2 below.

Sponsorship: As mentioned above, sub-contracted companies without a direct business relationship with CLT, will need to be either signed for by the prime company or department for which they are contracting (e.g. Bravo Plumbing for CLT Facilities will need to be signed for by the Facilities Department), 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 do not meet Authorized Signer responsibilities, including general negligence and badge accountability concerns.

Fingerprint Applications. Prior to being fingerprinted, 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 Crimine 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.

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 transfer.
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 will fill out an online CLT Onboarding and Change form that can be found on www.cltairport.com/business/credentialing. Any subcontractors needing change in access must

request this change through the primary contractor. Please allow up to three 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 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

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 of by reason of insanity, of any of the Disqualifying Crimes in any jurisdiction during the 10 years before the date of the individual's application for unescorted access authority, or while the individual has unescorted access authority.
b. **Determination of Arrest Status.** When a CHRC reveals that an individual seeking unescorted access authority, who is not covered by a certification from an Air Carrier, has been arrested for any disqualifying criminal offense without indicating a disposition, the ASC or his/her designee must investigate the arrest to determine whether it involves a Disqualifying Crime. If there is no disposition, or 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.

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.

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.

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.

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 one government issued photo-identification with their request. Replies will be sent the email address on record.

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.

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

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, 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.

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 those required of a Badge Holder. These responsibilities include, without limitation:

Security, Safety and Passenger Handling Program. Air Carriers must have a written, TSA approved, security, safety and passenger handling program.

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 employer 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 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.

6.1 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.

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 that has been granted for 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 replacement.
d. **Suspended:** is used to deactivate a Badge for a temporary period, off-site for an extended period, medical leave, Leave of absence, military deployment. suspended Badges will require a completed Badge request form to reactivate.
e. **Expired:** is a Badge that has not been renewed prior to midnight on the expiration date displayed on the Badge. An expired Badges of more than 30 days will require an applicant to start from the beginning of the badging process.

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

If a Badge 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 704-359-4012 after hours. Lost, stolen or destroyed Badge reports may be made by telephone, seven days a week, 24- hours a day. Upon notification of a lost, stolen, destroyed or unaccounted-for card, CLT will terminate all access associated with that Badge and note the Badge record accordingly.

Lost or Stolen Badge Limitation. Lost or stolen Badges can only be reported for active and current employees, not for employees that resigned, transferred, terminated or otherwise left

employment at the Airport and failed to return the CLT ID Badge. Badges belonging to former employees must be reported as terminated or unaccounted for.

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 request form and submit 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 in three years and may not receive subsequent Badges for any company until the lost Badge is returned or the fee paid.

Mandatory Return of Badges. Whenever employment status is terminated, 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 returned to the CLT ID Badging Office by the employer or employee.

Penalty for Failure to Return Badges. The employers will be charged $100 for any employee' 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 a unaccounted for Badge in their record, will need to return the Badge or pay 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.

Confiscation of Badges. CLT Access Media is the sole property of the Airport and it is the Airport User's responsibility, through their designated AS, to ensure the Access Media 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 Airport 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; tampering or interfering with the Airport's access control system; interrupting or disrupting airport operations; or damaging airport property.
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.

CLT's Responsibilities and Right to Audit. CLT is responsible for the control, accountability and issuance of CLT Badges. To accomplish these responsibilities, CLT reserves the right to audit Airport Users' Badge records at any time, without prior authorization or notification. The ASC or his/her designee will conduct an audit of all active Badges that allow access to the AOA, Sterile and/or Secure Areas annually, randomly or whenever there is a reason to suspect that the CLT Badge Identification System has been compromised; The audit will be initiated and completed in the Authorized Signer portal 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 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.

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 citation 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 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. **Badge Must be Used for 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 Badge 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 will result in permanent revocation of Badge.

c. **Badge 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. **Badge for Use during Designated Work Hours for Job-Related Purposes**. Badge holders may only access the Sterile Area during designated work hours and for job-related purposes, unless approved by the ASC. For approved entry outside of designated work hours, the employees are required to enter the Sterile Area through the security screening checkpoint, unless all the screening checkpoints are closed at the time.
e. **By-Passing Screening.** Badge holders traveling on commercial flights may not use CLT Access Media to bypass or escort others around the TSA security screening checkpoint process. Further, all Concessionaire employees are required to enter the Restricted Areas through a security screening checkpoint. **NOTE:** Violation of will result in Permanent revocation of Badge.
f. **Multiple companies.** Employees who work for multiple companies are required to access the airport and display the Badge for the employer for which they are currently on-site for.
g. **Random screening and searches.** Employees are subject to random screening and searches by the TSA 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.

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***. 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)*

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) is 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 citation.

7.4 Piggybacking and Tailgating Prohibited.

Badge holders must ensure that doors or gates that 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 and assuring that they get a green light on the card reader before proceeding.

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 gets 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 cited.

7.5 Challenge Responsibilities

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.

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; 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 citation 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)1 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 Suspicious Activity

All Badge holders must immediately report any 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 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, etc.

7.7 Escorting.

Any person with a CLT Badge with an "Escort" designation may escort under the following conditions:

a. The escort is for official business
b. Escorted person(s) not currently 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 Secured Area from Sterile Area only for business purposes, such as to 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) has 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 that has access to the area of escort
h. Escorted person(s) has 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. Escorted persons who get separated, must immediately stop; 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.

Note: Escorted person(s) and their items are the Escort's responsibility while under escort and can lead to citation where such actions are in violation of these requirements.

8 Other Access Requirements

8.1 Clear Bag Policy

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.

Clear Bag: Total dimensions cannot be more than 37 inches (H + W + D < 37"). The bag must allow visual observation of the contents and not be obstructed by logos, design, etc. Mesh bags, smoky, metallic and tinted bags are not allowed.

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. Opaque bags/items in the Sterile Area screened by TSA
b. Walmart, other supermarket plastic bags for food instead of a lunch bag, the size must be the same or smaller than the maximum dimensions for the lunch bag.
c. Airline employees utilizing the Known Crewmember portal (not SIDA Badge holders)
d. Employees arriving on a flight and starting their shift (must have a boarding pass)
e. Government employees on official duty; credentialed TSIs, LEOs
f. Small "clutch" purse <6.5 x 4.5"; has to be inside clear bag & is subject to search
g. Escorted persons – their escorts are responsible for ensuring no Prohibited Items are present
h. Airline Mechanics in uniform traveling on official business

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.

*For Clear Bag policy and Frequently Asked Questions (Visit cltairport.com/business/credentialing)

8.2 Vehicle Access Procedures

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, the company's name and/or logo visible, not faded and legible, affixed to both sides of the vehicle.
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 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 Secured Area or the AOA it is considered to be in the Secured Area or the AOA and subject to any relevant citations and penalties up to and including Permanent Revocation of the Badge based upon the citation issued.

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.

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.

8.3 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. 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 CLT Airside Operations or a CLT Airside Operations approved representative. Having a "DR" 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. Drivers of motor vehicles being escorted must stay with their motor vehicle until it leaves the Secured Area or the AOA.
e. The escorted vehicle must follow and stay with the vehicle providing escort at all times while under escort.
f. 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.
g. 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 CCTV Access Requirements

CLT's Video Management System ("VMS") is classified as containing Sensitive Security Information ("SSI"). Users of the VMS are granted access subject to compliance with the following:

a. The user can only access CLT's VMS to complete official work responsibilities.
b. The user is responsible for notifying the ASC, or designee if any unauthorized use of CLT's VMS is observed or reported.
c. The user must comply with all directives governing the use of the VMS.
d. 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 the VMS 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.
e. The user must log off when not using the VMS to avoid unauthorized use;
f. 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.
g. The user is prohibited from releasing any video, 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 will result in permanent revocation of the user's badge.

h. The user is prohibited from recording video of ay 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.
i. The user shall abide by all guidelines instituted by CLT.

CLT monitors the VMS 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 citation, up to and including permanent Badge revocation, revocation of VMS access and federal penalties.

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 citations, violations and possible consequences are as follows:

9.2 Severe Violations – Permanent Revocation

a. Loaning/Borrowing an ID Badge to/from Another Person (Revocation *of both person's Badges)*.
b. Loaning/Borrowing Security Keys to/from Another Person (Revocation *of both person's Badges)*.
c. Falsification, copying or reproduction of CLT Approved Access Media, application, or documentation for Credentialing purposes, and any other fraud.
d. Bringing in or possessing dangerous weapons, explosives, and/or ammunition on Airport property
e. Bypassing Screening - Employee access and Passenger screening
f. Sharing AS Portal login information.

g. Responding to the Disqualifying Crimes questions for the applicant.
h. Sharing login information for CCTV systems. (Section 8.4 d)
i. Unauthorized release of video surveillance footage. (Section 8.4 g)

9.3 Permanent Badge Revocation Hearing

For severe violations, 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 may take up to 30 days.

9.4 Infractions

a. Unauthorized Use of Access Point (Section 7.3)
b. Piggybacking or Tailgating (Section 7.4)
c. Escort Violations (Section 7.7 or 8.3)
d. Failure to Challenge and follow Challenge Procedures (Section 7.5)
e. Introducing or attempting to introduce Prohibited Items not required for work purposes, into the Sterile or Secured Areas (Section 7.3)
f. Leaving Prohibited Items in the Sterile or Secured Areas (Section 7.3)
g. Unauthorized bags in the Secured Area (Section 8.1)
h. Failure to Comply with Directives of Security, LEO or TSA Personnel (Section 6.1)
i. Failure to Secure an Access Point (Section 7.4)
j. Failure to comply with rules governing CCTV system usage (Section 8.4, except 8.4 d and g)
k. Authorized Signer Negligence (Section 5, except where noted that the penalty is permanent revocation of the AS badge)

A combination of any **three** or more Infractions within **three** years will result in **permanent revocation of the person's Badge.** If an employee does not commit another offense within **three** years, a future offense will be treated according to the rules as a **1st** offense.

9.5 Issuance of Citation

Once a violation of the security program has occurred, a citation 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.

Note: For severe violations, you may have your **Badge confiscated,** be escorted to the non-sterile or public area, and receive a citation pending a scheduled hearing.

9.6 Citation Penalties

A. **First offense**:
   a. ***Infractions:***
      i. Warning; or
      ii. Badge Confiscation/up to three days - SIDA re-training - minimum $100 Badge reactivation fee, for infractions listed in section 9.4.
   b. ***Severe Violations:***
      i. Permanent revocation of the Badge for severe violations listed in section 9.2.
      ii. Where mitigating circumstances apply, a Badge may be confiscated for a shorter duration instead of permanently revoked.

B. **Second offense within three years**:
   a. ***Infraction:***
      i. Badge Confiscation/up to seven days.
      ii. SIDA re-training with manager/supervisor
      iii. Minimum $200 Badge reactivation fee, for infractions listed in section 9.4
   b. ***Severe Violations***:
      i. Permanent revocation of the Badge for severe violations listed in section 9.2
      ii. Where mitigating circumstances apply, a Badge may be confiscated for a shorter duration instead of permanently revoked

C. **Third offense within three years**:
   a. Permanent revocation of Badge.

9.7 Appealing a Citation

After receipt of the citation, 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 Citation Review Board ("CRB"). All appeals must be submitted by email listed in the citation notification. The email address as of the date of publication is SecurityViolationsAppeals@cltairport.com.

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.

The CRB, 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 CRB disposition of the violation. The violator must coordinate with his or her employer to satisfy the requirements of the CRB's findings and penalties as applicable. The appeal process will typically take from seven to 30 days.

9.8 Appeal Review

Upon notification of the decision of the CRB, the violator has 30 days to appeal the decision in writing to the ASC. In case the ASC is not available, the violator will need to appeal to the Chief Operating Officer. The email address for this appeal will be provided in the letter with the decision of the CRB.

9.9 Airport User Fines and Penalties

Airport Users can be penalized for security violations as a company as well as holding Badge holders or 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 citation penalties, or continuous and/or habitual violations by Airport User employees.

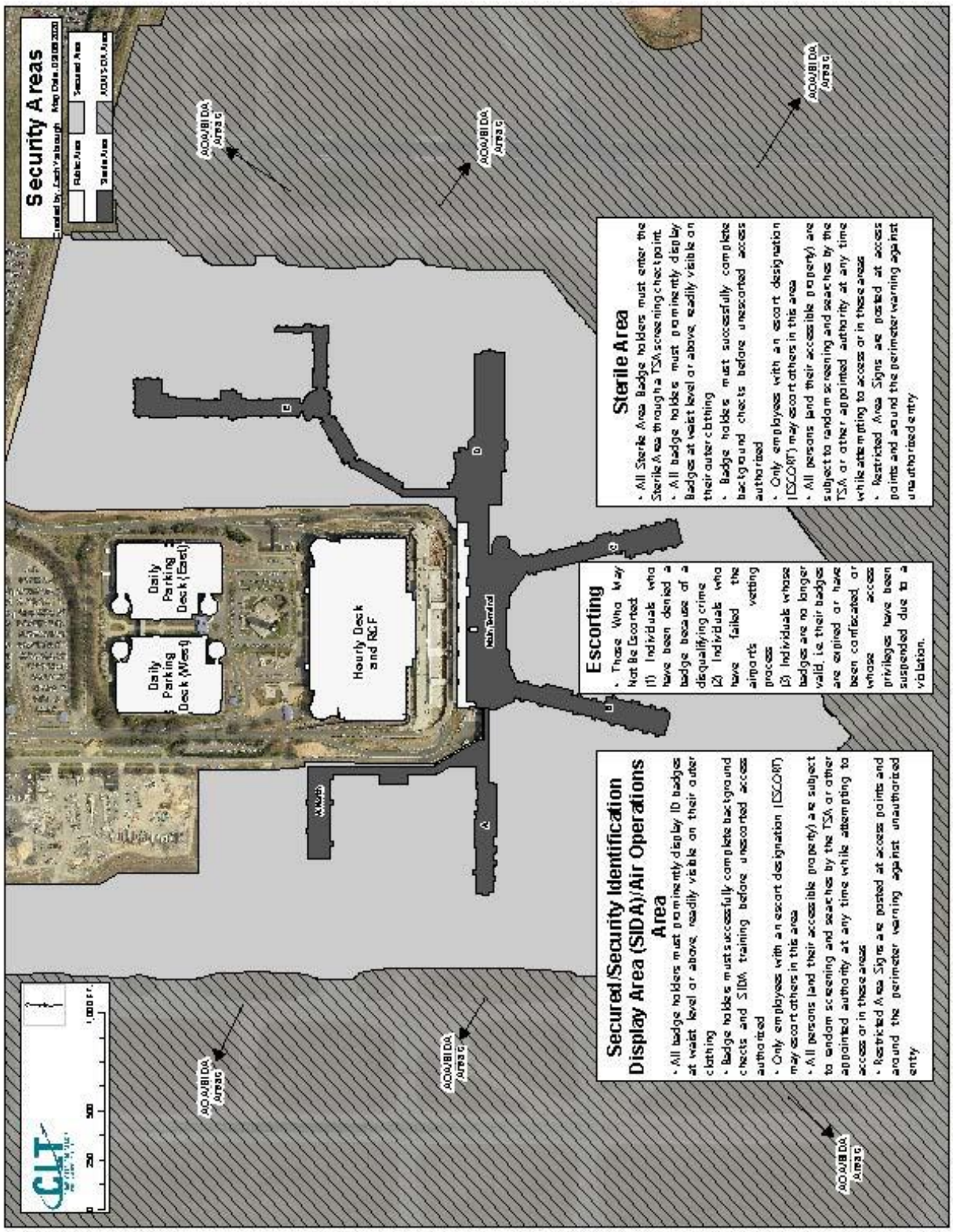
Fines or monetary penalties assessed against CLT by the TSA or other regulatory agency, after all appeals have been exhausted, for infractions or violations of applicable TSA regulations, may be passed on to the airline/tenant involved or equally assessed between the airline/tenant and CLT. CLT has the 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 citation following the appeal process set forth in Section 9.7

Appendices

Appendix 1


Security Areas
Public Area
Sterile Area
Secured Area
AOA/SIDA Area
Daily Parking Deck (East)
Daily Parking Deck (West)
Hourly Deck and RCF
Main Terminal
AOA/SIDA Area
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 in 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 airports 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 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
AOA/SIDA Area
AOA/SIDA Area
AOA/SIDA Area
AOA/SIDA Area
AOA/SIDA Area
CLT
0
250
500
1,000 Ft.

Appendix 2

Disqualifying Crimes

(1) Forgery of certificates, false marking of aircraft, and other aircraft registration violation, 49 U.S.C. 46306.
(2) Interference with air navigation, 49 U.S.C. 46308.
(3) Improper transportation of a 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 *Ramp Safety 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 Rules and Regulations, including provisions of Title 49, CFR, Parts 1540, 1542, and 1544 as applicable.

1. The following Security Violations will likely **result in immediate and permanent revocation** of a CLT SIDA badge; **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.*

2. **Multiple Badge holders -** In addition to the provisions in the Security Training Program and CLT Security Standards, employees that have been issues 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:** _____

3. 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

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

5. 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

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

7. **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).

8. 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.

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

10. 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.

11. 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 waist on the outer garment so as to be clearly visible.

12. 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 emergency notification number is 704-359-4012 located on the back of the CLT security identification badge.*

13. Each person must enter AOA and SIDA/Secured Area using their issued CLT security identification badge. 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, with the exception of Field Gate 1. At that gate the badge holder must verify that the vehicle has access and has taken control of the gate.

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

15. All lost, misplaced, or stolen CLT security identification badges or keys must be immediately reported to 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.

16. 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 license is suspended or expired the DR endorsement will be removed.

17. 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 to ensure 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.

18. CLT security identification badge holders may ONLY escort a person in the AOA, SIDA, Secured, or Sterile area if they are a designated authorized escort. The badge will reflect an approved escort with appropriate endorsement. 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.

19. **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 for assistance.

20. All CLT security identification badge holders must renew 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.

21. 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 will be issued. Use of an expired badge is a security violation and may result in denial of badge renewal, criminal and/or civil penalties.

22. 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.

23. 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.

24. 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.

25. 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.

26. 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.

27. Badge holders must comply with 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.

28. 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:** _____

Appendix 4

The following are examples of bags that are NOT allowed. They cotain logo, or a pattern. Only clear bags without logo or patterns comply with the policy: