Sports Venue Credentialing Guide

May 2012

Homeland Security

Sports Venue Credentialing Guide

Table of Contents

Introduction

This guide provides suggestions for developing and implementing credentialing procedures at public assembly venues that host professional sporting events. Venue owners, operators, and event organizers should use additional resources (e.g., law enforcement) when available to implement the procedures outlined in this guide.

The credentialing procedures delineated in this guide are presented for guidance purposes only; they are not a requirement under any regulation or legislation. In addition, due to the wide variation in the types, sizes, and locations of public assembly venues and the events held in these venues, not all suggested procedures will be relevant or applicable.

Photos for this Guide were generously provided by Major League Baseball (MLB), the National Football League (NFL), the U.S. Tennis Association (USTA), the U.S. Golf Association (USGA), and the U.S. Open.

1. Purpose

Credentialing serves as an access control process for individuals who desire access to or wish to move within a venue.

- The purpose for establishing a credentialing program is to control and restrict access to a venue, and provide venue management with information on those who have access.
- Credentialing can also be used to control and restrict vehicle movement within and around a venue.

2. General

The success of a credentialing program at public assembly venues that host professional sporting events relies on the combined efforts of the entire venue staff.

- For those instances when the sports team(s) or primary event sponsor does not own the venue, contractual agreements or operating procedures should be in place to create a credentialing program that meets the needs of all parties involved.
- The entry criteria into controlled/sensitive areas of the venue should be in writing and agreed upon in advance by the team, event sponsor, and the owner or operator of the venue.
- The credentialing program should be incorporated into the venue's operational security document and be reviewed by law enforcement and the sports leagues using the venue.

Success requires education and effective execution of the credentialing program to instill ownership, meet security goals, and provide a safe experience for all attendees.

- To be truly effective, all venue staff, not just those at the credentialing office or those manning the access control points, must accept accountability for the program's implementation.
- Ownership in the program must be instilled in all staff to empower them to report or correct credential misuse. Creating a "culture of responsibility" where exceptions to the credentialing program will not be tolerated by staff or attendees alike will enhance security of the event(s).

Clear guidance should be provided to the access control personnel for dealing with individuals trying to gain access without the proper credentials.

- Criteria for allowing individuals access to different parts of the venue should be clearly delineated (i.e., sports team equipment managers should be allowed access to the locker room, playing field, equipment storage areas, etc.).
- Criteria must be established for excluding individuals from controlled areas of the venue and from receiving credentials (e.g., general ticket holders from Very Important Persons (VIP) areas and dressing/locker rooms and/or event personnel from mechanical and administrative areas).

It is recommended each venue establish a written credentialing program commensurate with the complexity of the venue, the types of events held at the venue, and the available resources (e.g., funding or staffing).

The credentialing program should not only focus on event day and nonevent day access to the venue, but also address the various types of individuals accessing the venue (e.g., full-time staff, contractors, or event day employees and participants) and the timeframes associated with personnel access (e.g., full-time employee, contract/task specific, or daily/entire event).

The credentialing program should also identify who will approve or deny requests for credentials and include written access criteria for each controlled area of the venue to support the approval or denial process.

- Credential requests should be divided into categories or groups based on functions (e.g., concessions, ushers, visiting team, press, event personnel, and event attendees).
- Someone who has responsibility for or knowledge of the event (e.g., facility management, contracting officer, head of security, or head of concessions) should approve or disapprove individuals associated with the event to the credentialing office for final approval and processing.

The mechanics of the credentialing program are just as important as the access control aspects.

- Training for the credentialing program is important. The employee holding the credential as well as access control personnel should be trained in credential recognition, areas of access control, and the resolution of access control issues.
- Even though venue employees may have credentials that allow them general venue access, they should know what areas of the venue they cannot access during an event as well as when not to display or wear their credentials (e.g., in areas designated for paying event customers or offsite).
- Procedures should be in place for reporting and replacing lost or stolen credentials as well as denying access to the barcode assigned to the credential, if applicable.
- Individuals found in the venue without credentials should be questioned and escorted to the credentialing office/security office where a determination will be made of their access status by the security manager responsible for the event.
- Credentials should be made out of materials that contain anti-counterfeiting technology (e.g., holograms) to discourage forgeries.
- Credentials for specific events should contain event name, date/time, personnel type information, and/or coding.
- Credentials should be clearly visible at all times and presented to access control personnel upon request.
- Credentials should be returned as part of the employee out processing procedures when employment is terminated at the venue (either by employee or by management).

3. Credentialing Office

The credentialing office should be the focal point for the processing of all credentials associated with access to the venue.

- The head of the credentialing office should be responsible for granting or denying all requests for credentials based on the guidance provided by the security manager responsible for the event.
- All nonevent and event credentials should be processed through the credentialing office.
- Any issues concerning credentialing should be adjudicated at the credentialing office.
- If employed, venue-created photo identifications (ID) should be processed at the credentialing office.
- If the venue's policy requires a person to leave a government-issued ID (e.g., driver's license) when they pick up their event credential, the collected IDs should be stored in a secure location within the credentialing office.

Figure 1: Credentialing Office (USTA)

- The location where credentials are processed should be located externally or on the perimeter of the venue in order to allow noncredential individuals to be processed without entering the area(s) of the venue requiring credentials.
- The credentialing office should process credentials for both nonevent and event day access.
- Operations of the credentialing office may be performed by venue staff or by a contracted agency. The operations should be scalable to accommodate nonevent days and various sized events as nonevent credentialing could be performed by venue employees, while contractors may perform event credentialing because of its size and complexity.
- Personal information required for credentialing should be protected and stored in a database with cyber security systems in place. The sophistication of the database should be commensurate with the credentialing program (e.g., venue-created photo IDs) and access control (e.g., swipe cards).

4. Nonevent Day Procedures

On nonevent days, access to the venue should be restricted to designated entrances based on job function (e.g., venue personnel, contractor, media, and event staff).

Figure 2: Security Desk (NFL)

- Security and access control personnel assigned to entrances should ensure that only those individuals displaying proper credentials for that particular access point are permitted entry.
- Each credential should be thoroughly checked prior to granting access. This includes touching and reviewing the credential, and if the credential has a picture, then confirming that the credential holder matches the person in the credential's picture. If the credential is a name-only credential, it may be necessary to confirm the person's identity by requesting a second ID (e.g., drivers license or passport) to confirm that the credential holder is actually the confirmed user.
- Access control points should have a "Sample Credential Board" (such as the one illustrated in figure 3 below) that clearly identifies which credentials have access to each entrance.

An **Organizational Chart** should be developed (see table 1 under section 5, Event Day) that identifies all roles and job responsibilities of nonevent individuals (e.g., maintenance, engineering, or administration).

- Timeframes (e.g., full-time, part-time, and event) for accomplishing those job responsibilities should be identified.
- The chart should define areas of the venue where activities associated with roles and job responsibilities take place (e.g., full-time employees in "front office," full-time operations in "engineering areas," or contractor working in specific area(s)).
- The chart should identify the types of employees (e.g., full-time, event day, or contractor staff), and work status of employees (e.g., full-time, part-time, or event specific).

Figure 3: Sample Credential Board (MLB)

- Consider whether or not creating daily spreadsheets from the database that shows locations of individuals in the venue is a viable option.
- Access to sensitive areas of the venue (e.g., information technology services, communications, finance, or electrical equipment) should be controlled through the use of swipe card credentials and keys.

4.1   Full-time and part-time venue employees should have individual credentials that clearly identify the user as a venue employee.

- Based on the sophistication of the credentialing system employed at the venue, full-time or part-time venue employees' credentials should include photo IDs and have swipe or proximity card access capabilities when applicable.
- Each employee should fill out a credential application form that contains the terms and conditions for using the credential, as well as pass a background check commensurate with their job functions (e.g., some positions may require substance abuse history and others may require a pre-employment credit report), either conducted by the venue or the contracting company, (refer to venue's background check procedures) prior to being issued a credential.

4.2   Full-time contractor support personnel may use the same credential as full-time venue employees, designated as a contractor by a "CTR" on the credential, or have their own credentials.

- Each full-time contractor should fill out a credential application form that contains the terms and conditions for using the credential, as well as pass a background check commensurate with their job functions (e.g., some positions may require substance abuse history and others may require a pre-employment credit report), either conducted by the venue or the contracting company, (refer to venue's background check procedures) prior to being issued a credential.

4.3   Temporary contractors should be issued credentials that are work order-specific, indicate a time frame for work to be performed, and designate the area(s) of access (e.g., escorted or granted).

- Each temporary contractor should fill out a credential application form prior to employment that contains the terms and conditions for using the credential, as well as pass a background check commensurate with their job functions (either conducted by the venue or the contracting company – refer to venue's background check procedures) prior to being issued a credential.
- Temporary contractors should be issued their credentials on a daily basis.
- Temporary contractors should fill out information on a contractor log sheet, sign in and out, and return their credentials each day before exiting the venue.
- Temporary contractors' credentials should be clearly visible and presented to access control personnel upon request.
- Control of temporary contractors' credentials can be achieved by requiring the contractor to turn in a government-issued ID (e.g., driver's license or passport) when issued a temporary daily credential and receive the ID back when the daily credential is returned.

4.4 **Employees and contractors** should have their credentials visible at all times while in the venue and present them to access control personnel upon request.

- Employees and contractors should not wear or display their credentials outside of the venue or venue grounds.
- Employees and contractors should know the areas within the venue where they do or do not have access, where they can or cannot wear their credentials (e.g., areas designated for paying customers), as well as the proper handling of credentials to prevent their theft.
- When possible, employees and contractors should be provided parking in a designated nonaccess controlled area. Vehicles entering an access control area should be searched and a parking pass/window sticker issued (refer to a venue's specific parking procedures).

4.5 **Visitors** (i.e., individuals not employed by the venue who are at the venue for meetings, tours, etc.) should be provided general or nonevent parking close to an entrance designated as the visitor's entrance.

- If general or nonevent parking is not available, then a visitor's name should be on an approved parking list for validation by access control personnel.
- Visitor's vehicles entering an access control area should be searched and parking pass/window sticker issued (refer to venue's parking procedures) prior to entering the area.

Depending on the sophistication of the credentialing system employed at the venue, visitors or the visitors' point of contact (POC) at the venue should fill out and submit a visitor request form prior to the visitor's arrival at the venue.

- Upon arrival, the visitor should provide information on a visitors log sheet (e.g., name, company, purpose, person visiting, badge number, and sign in and out time), go through any personal and bag screening or searches, and provide ID verification prior to being issued a temporary credential.
- The visitor's POC should sign on the visitor log sheet the time the visitor enters the venue as well as the time the visitor exits the venue.
- The POC should escort the visitor during the entire visit.
- Credentials should not be issued to visitors until receiving verification from a point of contact within the venue.
- The visitor's credential can be pre-numbered and entered on the visitor log sheet, a day-specific self-expiring credential with the date indicated on the credential, or a numbered photo ID.
- Ensure that passes are returned to security by all persons exiting the venue. As an incentive to returning the credential and following the appropriate sign out procedures, the venue can require the visitor to provide a government-issued photo ID (e.g., driver's license) to be held by the security office until the visitor leaves the venue for the day.

- All individuals who do not return credentials to the credential office should be identified, security personnel should be notified, and if necessary, those credentials should be deactivated.

Visitors who are not approved for credentialing should be refused entry, and asked to leave the venue property.

4.6   Tour groups visiting the venue should follow the same credentialing procedures employed for visitors.

- A visitor log sheet should be created for the tour group.
- A POC should be responsible for obtaining required credentialing information, submitting this information to the credentialing office for processing, and collecting the credentials at the end of the tour.
- An appropriate number of escorts should accompany the tour group to ensure everyone stays together in the group.
- The relinquishing of a government issued photo ID by members of a tour group should be conducted at the credentialing office.

4.7   Deliveries should be scheduled and approved ahead of time by the appropriate point of contact (refer to the venue's delivery/shipment procedures).

- All deliveries should be made to designated areas (e.g., loading docks) at the venue.
- Drivers should present a government-issued photo ID upon entering the venue.
- Delivery vehicles left unattended should be inspected and issued a parking pass/window sticker.
- Drivers who make routine deliveries (e.g., mail or concessions) and who deliver items beyond the loading dock area (e.g., inside the access control area) should be issued a credential in accordance with the procedures used for temporary contractors and escorted during the delivery.

Figure 4: Deliveries (USTA)

Temporary contractor vehicles, equipment vehicles, and tour buses parked within the access control area should be inspected, issued a parking pass/window sticker, and parked in designated areas based on work being performed (refer to venue's parking procedures).

5. Event Day(s)

Similar to the nonevent day credentialing process, event day credentialing should be based on each individual's job function (e.g., employee, event staff, or attendee) at the venue and areas of granted access. Unlike nonevent days, access control is greatly expanded to include many categories of individuals and locations that might not be controlled during nonevent days (e.g., locker rooms, operations and service areas, or press boxes).

Development of an organizational chart (table 1) that identifies individuals' job functions, associated areas of access, and desired access restrictions during an event can help to enhance a credentialing scheme that reflects the desired access control during an event. A similar chart can be created for nonevent days if desired.

Credentials should display information on areas of access, as well as show the timeframe for which the credential is valid.

- Full time employees and contractors may have credentials that are in effect for a number of years with the expiration date visible on the credential.
- Part time employees may have credentials that display the end date of the contract, work order, or event season (e.g., baseball season, concert, and theatrical series).
- Event staff and participants may have credentials that expire on a specific day of the event or are valid throughout the entire event.

Sports Venue Credentialing Guide

Table 1: Example Chart Identifying Staff Functions with Specific Access Areas

	Critical, most controlled areas		Controlled, operational areas								General access areas				Public access controlled areas
	Administration[1]	Playing/Event Area[2]	Operations[3]	Services Areas[4]	Security[5]	Response[6]	Media[7]	Players/Performer	Garage	Loading Dock	General Admissions	Seating Areas[8]	Concessions/ Restaurants	Parking	Club/Box Seats/ Executive[9]
Administration[A]	X	X	X	X	X				X					X	
Operations[B]	X	X	X	X	X				X	X				X	
Concessions/Vendors[C]												X			
Safety and Health[D]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Security[E]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Media[F]							X								
Field photographers TV camera		X					X								
Patrons[G]											X	X	X	X	
Officials[H]		X						X							
Ushers											X	X			X
Teams/ participants		X						X							
Event support staff[I]		X							X	X					
Guest/family		X						X							X
VIPs															X

[1] Administration ("front office," public affairs, event planning, ticketing, mailroom)
[2] Players/performers area (locker rooms, family rooms, dressing rooms)
[3] Operations (HVAC, boilers/heating/cooling devices, auxiliary power, general storage, exhibit hall(s), communications, water/fire pump room, oil/fuel storage, machine/engineering)
[4] Service areas (storage, kitchens, preparation, commissary)
[5] Security (command center, CCTV monitoring, containment, briefing room)
[6] Response (emergency response, fire, clinic)
[7] Media (press box, reporters' room, and interview rooms)
[8] Seating areas (ticketed seating)
[9] Club/Executive areas (ticketed seating)

[A] Administration ("front office," league)
[B] Operations (engineering, IT, daily operations)
[C] Concessions and vendors (preparation, serving, sales)
[D] Safety and Health (emergency response, safety)
[E] Security (contracted, local/State police, National Guard)
[F] Media (national, local, league)
[G] Patrons (general admission, suites/club level)
[H] Officials (referees, judges, league)
[I] Event support staff (equipment, mechanics, pit crews, coaching staff)

6. Creating Credentials

A well designed credentialing program is composed of many components.

- A credentialing scheme that is visually easy to discern and simple to use, yet difficult to falsify.
- If possible provide a hologram or other protective measure on the credential to reduce the potential for counterfeiting.
- Simplify the credentialing process by indicating areas of access by numbers, letters or symbols, and color-coding by event function.
- Design and color-code the credentials to ensure they are substantially different from those used at previous events or in prior seasons or years.
- Sequentially number credentials and maintain a record of each person issued a credential for control purposes.
- Provide important phone numbers (e.g., security or emergency response) on the back of the credential along with important rights and restrictions of the user.
- Implement a program for reporting and deactivating lost credentials.
- Provide all credentialed individuals with operations security training.
- Revoke credentials if worn offsite and during nonworking or nonevent hours if used to access areas unofficially.
- If possible create a credential that is "user-specific" so that the credential is nontransferable (e.g., photo of the user).
- If possible, during an event, use photo credentials for access to the most restricted areas.
- In some instances the venue may not allow full-time employees to use their badges during event days (e.g., in order to limit the number or types of employees at the event). Instead, the venue may require venue personnel (e.g., full-time employees or contractors) to obtain an event credential following the same procedure(s) as other event staff and attendees.
- Develop a procedure to destroy or deactivate past event or out-of-use credentials.

7. Requesting Credentials

Develop a credential request form containing personal information, function, areas of access, timeframe, terms and conditions, and releases for all credential requests.

- Penalties for violations of the credentialing program should be clearly stated on the request form.
- Event staff and attendees should complete and sign the form prior to the event or at the credentialing office at the venue.
- Out-of-town individuals such as visiting teams, performers, friends and family, exhibitors, national sports league staff, media, and VIPs should submit credentialing requests electronically via fax or email.

The head of the credentialing office should be responsible for granting or denying all requests for credentials based on the guidance provided by the security manager responsible for the event.

- Develop written access criteria for each controlled area to support the approval or denial process.
- Credential requests should be divided into categories or groups based on functions (e.g., concessions, ushers, visiting team, event staff, and event attendees).
- The recommendation for approval or disapproval should be made by someone who has responsibility for the event or group (e.g., contracting officer, head of security, or head of concessions) during the event and this recommendation should be provided to the credentialing office for final processing.
- Individuals requesting credentials should be notified of the action taken on their behalf (either approved or denied) via email or postal mail. A formal justification for disapproval should be provided as well.

Unless other arrangements have been made (e.g., a designated individual obtains a number of credentials for a functional group), individuals requesting credentials should appear in person at the credentialing office and present a government-issued photo ID (driver's license or passport) with the name on the ID matching the name on the credential in order to obtain their credential.

The credentialing program should be flexible in order to coordinate national events credentialing (e.g., professional sports leagues, national associations, or national touring groups) with venue specific credentialing. As an example, the professional sports leagues may issue season passes to the media, league staff, and the regular traveling party for each team. Season passes should contain a photo ID for quick identification purposes. Based on the agreements between the sports league and the venue, these season passes may allow the user access to all venues where the league holds events.

- These season passes should be integrated with the venue's specific credentialing program.
- The home team or venue should issue day or event passes in addition to season passes in order to determine levels of access and to record attendance on an event-by-event basis.
- A similar process may be employed for media personnel who accompany a team on away games for the entire season.

Credentialing arrangements should be made between the venue and the visiting teams and event performers or participants in order to process all essential individuals at one time. This would include not only individual credentials, but also the necessary controlled parking access for team buses, media vehicles, individual team members, and family vehicles.

As a best practice, the venue should establish a maximum number of guest and/or family credentials allowed by team members, VIPs, and season-ticket holders with exceptions granted in special circumstances only. VIPs, team members, and performers should be instructed in the importance of the venue's credentialing program and that abuses can result in the cancellation or reduction in the number of credentials issued.

For those instances when access is required after a badge or credential has been issued, a supplemental credential (e.g., a colored wristband) can be issued to an individual for access to a particular event or area of the venue.

8. Using Credentials

Credentials should be worn at all times and be clearly displayed within the controlled areas.

- All team members should be issued credentials to be worn inside the venue during warm-up and practice.
- When not in a designated controlled area, players, officials, and performers should be required to wear a credential to enter other controlled areas within the venue.
- Nonuniformed players should be provided an event day credential to wear during the event.

To assist with access control, display credential boards or access documentation guides (as illustrated in figure 5 below) at all access control points.

- Access control personnel should be trained in recognizing the credentials that are allowed within their specific controlled area, in identifying counterfeit credentials, in the procedures for denying entry, and in confiscating credentials.
- There should be zero tolerance for allowing an individual into a controlled area without the proper credential.
- All venue staff should enforce the credentialing program and report abuses to venue security.

Figure 5: Credential Board (USTA)

- Specific procedures should be developed for use by access control personnel and all venue employees for notifying security of violations to the credentialing program.

Credentialing of local law enforcement should be considered during an event. It is important for event and security staff to be able to identify law enforcement whether in uniform, plain clothes, or undercover. It also allows the event organizers to identify those officers who are there on official duty and those who are not.

- Law enforcement officers should conform to the same credentialing requirements as all other event attendees (e.g., readily visible, proper access marking, and wear only during official business).
- If responding to an incident, plain clothes and undercover officers should have an arm band or other credential to clearly identify them as law enforcement officers to event security staff and other law enforcement personnel.

Because of their duties and job responsibilities (i.e., game officials, players, performers, security, emergency management, etc.) at the venue, certain individuals may not wear event credentials on the days of the events.

- Performers, players, and officials in uniform should be the only persons not required to wear a credential.
- Create a roster that identifies the individuals by name and their job responsibilities that do not require credentials (e.g., players/officials in uniform) within specific controlled areas (e.g., playing field, race track, pit areas, or back of house).
- These individuals may enter the venue by way of a controlled, nonpublic access point (e.g., teams and/or performer's parking lot).
- Each individual should be identified by a government-issued photo ID and confirmed by the roster.

Figure 6: Arm Band (USGA)

Venues should consider assigning a security staff member to each team's locker room doors to ensure that only approved persons are admitted.

- Persons other than players, coaches, credentialed team staff, and working media should be prohibited from entering the locker rooms.
- Escorts should be provided when necessary.

9. Credentialing Event Equipment

When conducting bag inspections, apply color-coded tags to all bags belonging to media, officials, individual team members, performers, and employees.

- The color-coded tags should be changed for each event, and all previous tags must be removed from the bag(s) before affixing the current color-coded security tag.

For sporting events, the visiting team's equipment should both be inspected and tagged or have an agreement with the visiting team that they have performed an inspection of the equipment and maintained control and custody of the equipment.

- Assign responsibility to the designated team security person for ensuring that the carry-on bags, luggage, and equipment of the visiting team, its staff, and the traveling party have been inspected and tagged (refer to venue's bag inspection procedures).
- Media or stage equipment, sets, and exhibitors' containers should be inspected and tagged in a similar manner.

10. Vehicle Credentialing

The credentialing program should consider inspecting and issuing parking passes/window stickers for all vehicles allowed inside the controlled perimeter.

- Multiple means (i.e., through the venue web site, on the back of tickets, etc.) should be employed to inform event participants that all vehicles entering controlled areas are subject to screening and inspection procedures.
- Develop and use a parking request form to allow access to controlled parking areas. The form should contain information on the vehicle to be parked (e.g., make, model, or year), the driver of the vehicle, the reason for parking the vehicle (e.g., team member's vehicle), and the area where the vehicle will be parked (e.g., lot A).
- Information on the timeframe for parking (e.g., not on event day, before, event, or during event), and any venue terms and conditions for parking (e.g., not responsible for items left in the vehicle) should also be included on the parking request form.

Figure 7: Courtesy vehicle (USGA)

Figure 8: Shuttle bus stickers (USGA)

- Have individuals submit the signed parking request form along with the credential request form to the credentialing office prior to the event.
- Out of town individuals (e.g., visiting team, performers, friends and family, exhibitors, national sports league staff, media, or VIPs) should be able to submit the forms electronically via fax or via email.
- Courtesy vehicles used by players/participants should display a unique parking pass/window sticker specific to the individual assigned the vehicle and the parking location. This information should be verified by event security staff prior to allowing the vehicle entrance into the controlled perimeter.
- Shuttle buses/vans should display a unique sticker or marking for each daily event that indicates the vehicle has been inspected and is allowed within specific areas of the controlled perimeter.

- Identify those individuals who will approve or deny requests for access to controlled parking and develop written access criteria for each controlled parking area to support the approval or denial process. Parking areas should be divided into categories based on functions (e.g., home team, visiting team, performers, concessions, event staff, and VIPs).
- Parking approval or disapproval should be made by someone who has responsibility for the individuals parking in the controlled areas (e.g., team front office, league representatives, event promoter, head of security, and head of concessions) during the event.
- Individuals requesting controlled parking access should be notified of the action taken on their request (approval or denial) by email or postal mail. A formal justification for disapproval or revocation should be provided.

Whenever possible the number of vehicles that can park within the secure perimeter next to or under the venue should be limited. Consider developing a vehicle access control chart that identifies the parking areas associated with the event functions (e.g., team parking near team locker rooms, and refrigeration trucks near food storage and preparation areas). Areas to consider may include:

- Loading dock area(s);
- Media vehicle area(s);
- Team buses;
- Emergency Medical Services area(s);
- Infield area(s);
- Shuttle bus drop off/pickup points;
- Contestants' Recreational Vehicles area(s);
- Team, officials, area(s);
- Garage area(s); and
- VIP/family area(s).

Individuals and groups (e.g., teams, performer, or pit crews) requesting credentials and access to controlled parking should be notified of the approval or denial of their request and informed of the process for obtaining their credential and parking pass/window sticker.

- In the days prior to an event, individuals may park in the visitor's parking area and obtain their credential and parking pass/window sticker from the credentialing office.
- Each vehicle should be logged in as to their access time, location, driver's license information, contact information, and parking location as part of the issuance process for a parking pass/window sticker.
- On event days, controlled parking access control personnel should have a roster containing the names of individuals, or groups and vehicle information (e.g., make of vehicle, or license plate) approved for the controlled parking area.
- A valid government-issued photo ID should be presented before a parking pass/window sticker is issued and access is granted.
- Vehicle searches may be conducted based on the venue's protective measures procedures.

- Once in the controlled access parking area, individuals may obtain their credentials either from the credentialing office, or from another access control location associated with the parking area and event functions.

Depending on the space available within the controlled parking area, season parking passes/window stickers may be issued to select individuals (e.g., team members and family, officials, season ticket holders, and VIPs).

11. End of Event Credentialing Activities

The venue should employ the same level of concern for unauthorized entry into the venue while spectators or patrons are still present.

- Ensure that adequate security and event staff members are present to deal with the large crowds exiting the venue at one time, and that they pay particular attention to those individuals wishing to enter the venue at the end of an event.
- Collect all temporary credentials at all controlled access points and the credentialing office.
- Cross-check returned temporary credentials against the credentialing database to identify credentials not returned.
- Use this information when issuing credentials in the future to reinforce the importance of the credentialing program.
- Continued failure to return credentials could result in the forfeiting of credentials.
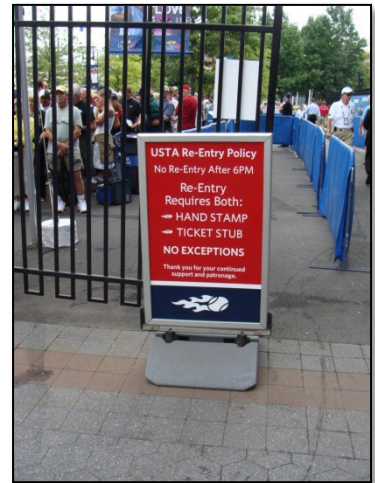- Destroy or deactivate credentials no longer valid or in use.

Figure 9: Re-entry Requirements (USTA)

An After Action Review of the credentialing process is an important component of the emergency security and safety process.

- This review should critique what credentialing issues or incidents occurred during the sporting event, how they were resolved and what changes might be made as a result of issue/incident.
- It should also include an assessment of what worked well, what could be improved upon, and what lessons were learned.
- Lessons learned should be identified in the report, and a list of recommendations should be compiled for implementation.

References

- *Arena Security Procedures and Guidelines*, National Basketball Association, 2008.

- *Best Practices for Stadium Security*, National Football League, 2002.

- *Best Practice Planning Guide for Arenas, Stadiums, and Amphitheaters*. International Association of Assembly Managers, 2003.

- *2009 Pro Motocross Credential Policy*, May 2009.

- *Protective Measures Guide for U.S. Sports Leagues*, U.S. Department of Homeland Security, 2008.

- *Recommendations for Arena Security*, revised, National Hockey League, 2005.

- *Security and Safety Guideline Reference Manual, Version 1.0.*, Ingersoll Rand Security Technologies, NASCAR, Inc., 2006.

- *Security Procedures Manual*, Rodriguez, Michael J., U.S. Tennis Association, National Tennis Center, 2005.

- *Smithsonian Institution Credentials* (OPS-56), July 2003.

- *Team Security Survey*, updated, Major League Soccer. 2006.