BEST PRACTICES FOR NIGHTLIFE ESTABLISHMENTS

NYPD

NYC HOSPITALITY™ ALLIANCE

DEVELOPED IN COOPERATION WITH THE

NEW YORK CITY POLICE DEPARTMENT
NEW YORK CITY HOSPITALITY ALLIANCE

THIRD EDITION 2018

BEST PRACTICES FOR NIGHTLIFE ESTABLISHMENTS

TABLE OF CONTENTS

Forward to the 3rd Edition

This 3rd Edition of Best Practices for Nightlife Establishments, published March 2018, reflects an effort by the New York City Hospitality Alliance and the New York City Police Department to continue our tradition of working collaboratively to improve the safety and security of New York City's famous nightlife. We are proud that many jurisdictions have chosen to use our guide as a basis for their own, and we encourage this use. This 3rd Edition adds new materials to this volume which reflect the newest developments in the nightlife industry.

BEST PRACTICES FOR NIGHTLIFE ESTABLISHMENTS

DEVELOPING A SAFE NIGHTLIFE ATMOSPHERE

The goal of this document is to assist nightlife owners and managers in maintaining bars, lounges and clubs which are safe and free from illegal activity including: drug sales, underage drinking, overconsumption of alcohol, violence, prostitution, assaults, and sex offenses.

The NYPD, together with the New York City Hospitality Alliance, has developed these guidelines as suggested ways to achieve that goal. They are meant to serve as a general road map for owners and managers, not as a list of laws applicable to all establishments or all situations.

Also included are separate sections which address how to respond to a serious criminal incident and what nightlife establishment operators should know about counterterrorism threats and preparedness. Nightlife professionals should use their knowledge, experience, and judgment to adapt these guidelines for their specific establishment.

SECURITY

1. As a general guideline, the security guard to patron ratio should remain one (1) security guard for every seventy-five (75) patrons. Discretion should be used by management to employ additional security guards based on the event or crowd to ensure safety and lawfulness.

2. Under New York State law, if the establishment uses a third party security guard company rather than proprietary security guards, the security guard company must be licensed by the NYS Department of State. In addition, all security guards utilized must be licensed by the NYS Department of State. If you hire directly in-house security guards, the business must register with the NYS Department of State.

3. Security guards should be trained in communication and de-escalation techniques, recognition of terrorist indicators and behaviors, and criminal and terrorist pattern recognition. All employees of the establishment should receive training in the establishment's counter-terrorism and emergency plans.

4. Establishment policy should mandate that security personnel separate and remove all potentially violent patrons in a lawful manner which is designed to prevent continuation of the violent activity inside or outside the club. Establishments must call 911 to report criminal activity and may call 911 or otherwise notify police for assistance in potentially violent circumstances. Similarly, 911 must be called to report medical emergencies such as drug overdoses.

5. It is recommended that for every five (5) security guards there be one (1) security supervisor to ensure a maximum span of control of one to five.

6. It is recommended that security guards be distinctively and uniformly attired. This will serve to make them very easily identifiable to patrons, potential criminals, and first responders.

7. It is recommended that security guards be spread throughout the establishment and not just at the door.

8. Coat checks should include the customer's ability to check bags. Customers should be encouraged to check coats and bags so as to avoid theft. It is recommended that establishments install anti-theft environmental designs such as drawers, shelves and hooks for customers who choose not to check bags. Order should be maintained in the coat check area, especially at closing time.

9. Perpetrators should be detained by security through lawful means. Witnesses should be encouraged to wait for the police to arrive so that they may assist in the investigation. At a minimum, they should be asked to provide their contact information so that they may be contacted by the police in the future. They should also be encouraged to make a statement to establishment personnel regarding the incident. Additionally, establishments should act as complainants in appropriate cases.

10. Establishments should encourage employee witnesses to go to court to testify and pay wages to them for their time.

11. Digital video of any unlawful act and any act which may result in litigation should be identified and preserved. This video should also be provided to the NYPD.

12. Identifying information on ejected and/or arrested patrons should be retained in a "banned list" database. These patrons should not be allowed subsequent re-entry.

13. It is recommended that properly working and maintained digital cameras be mounted in front of the establishment (both inside and outside), at all entry doors and outside the bathroom doors.

14. It is helpful to learn if all of these efforts are working. To that end, establishments should hire an independent security consultant to ensure club security and adherence to other laws and policies, including laws prohibiting sales to minors.

15. Spot checks of employees should be conducted to ensure compliance with establishment policies and applicable laws and rules, including integrity tests for false ID and underage sales.

16. Ensure that levels of lighting inside and outside the establishment are sufficient for observation by security, and effective video recording.

17. Customers awaiting admission should stand in a line that does not block the sidewalk. All individuals on admission lines should be informed that if they are not orderly, they will not be admitted. Individuals who will not be admitted should be encouraged to leave the area.

18. At closing, security should ensure orderliness while patrons are exiting the establishment.

19. If metal detectors are used, every person entering the establishment should be checked with the metal detector in accordance with establishment policy. VIP's, DJ's, promoters, entourages, etc. should not receive special treatment and should be subjected to a metal detector check.

20. Establishments should safeguard evidence connected with commission of a crime on the premises and should maintain the integrity of any crime scene. See the section on "The Crime Scene", below.

21. Management should know and make readily available to managerial employees the telephone number of the local precinct and the name of the applicable Neighborhood Coordination Officer (NCO's).

INTOXICATION

1. State law and common sense prohibit a nightlife establishment from serving alcohol to a person who is visibly intoxicated, or permitting someone else to serve the intoxicated person. It is in the best interest of everyone involved to prevent the kinds of behavior which are associated with intoxicated patrons and all employees should be highly aware of the signs of intoxication including:

    a. Speech that is slurred, thick, confused, abusive, profane, antagonistic or incoherent
    b. Appearance in disarray, clothing stained
    c. Balance unsteady, or body swaying, using a wall or furniture to maintain balance
    d. Face pale or flushed
    e. Eyes bloodshot, red, or puffy
    f. Fumbling or dropping of glass, ID, cash, etc., or misjudging distance
    g. Unusual physiological symptoms, e.g., vomiting, excessive hiccupping, losing focus, sleepy or fainting

2. Ensure that all employees maintain continual awareness of the level of intoxication of patrons, as well as whether individuals are buying drinks for others who may have been cut off.

SEXUAL ASSAULTS

1. Although a sexual assault may not occur within a nightlife establishment itself, management and employees can help to prevent their premises from being exploited by sexual predators who may seek to take advantage of vulnerable patrons. Alcohol consumption can be a strong contributing factor to the loss of judgment and failure to perceive danger which can lead to a tragedy.

2. Employees should be attuned to behavior that seems overly familiar, aggressive, or seductive. Potential attackers are especially drawn to victims who are younger and visibly impaired or intoxicated. The predator may initiate contact in a nightlife establishment, purchase drinks for the potential victim, display romantic interest, and attempt to convince the victim to leave under false pretenses.

3. Establishment personnel should offer to call a vulnerable or impaired person a cab or otherwise watch as patrons leave to see if they seem to be able to navigate safely. Security personnel at the door or maintaining order outside are well positioned to observe when patrons leave. Note that predators may seek to get victims drunk or drugged, encourage them to get some air, and then pull up in a car or hail a cab to take them away.

4. Because of their vulnerability, intoxicated people should not be allowed to get into a for-hire vehicle alone. A friend or family member should accompany the intoxicated person to their destination.

5. If establishment personnel sense that something is awry when a patron leaves with a suspicious person, they should make it clear that they have noted the departure and communicate this to the suspicious person. For example, by commenting on an item of clothing, or asking if they need any help getting a cab. If possible, it would be a good idea to make a note of the circumstances, descriptions of the parties, and any other information that could become relevant at a later time. In some instances, a cell phone picture may be taken of the suspicious person, optimally together with the potential victim. The knowledge that a picture exists may be enough to discourage a future sexual assault.

6. Encourage groups to designate one person as a chaperone, perhaps identified by a wristband, who could be served non-alcoholic beverages at a discount for the night.

7. In order to prevent assaults from occurring in the establishment, as mentioned above, it is recommended that digital cameras be maintained both inside and

outside. These cameras should be monitored whenever the establishment is open to the public. All storage areas and other restricted areas should be kept locked and secured, as any closed, darkened area presents a potential danger. Establishments should consider employing a restroom attendant.

8. Support staff, including porters, barbacks, busboys, and kitchen staff, should be encouraged to be aware of patron behavior and possible dangers of sexual assault, especially as these employees work in or pass through areas which are dark or restricted. They should be instructed to immediately report any suspicious or problematic behavior to a supervisor or manager. Training sessions to identify potential sexual assault behaviors should be conducted with all support staff.

9. Cameras in front of the location should be used to record video of patrons leaving the location and entering vehicles. This will help to discourage criminals posing as legitimate for-hire vehicle operators. To maximize the deterrent effect of these cameras, signs should be posted in front of the location informing people in this area that their actions are under video surveillance. This video should be maintained for at least 30 days. Additionally, if the establishment provides a for-hire vehicle for a patron, a livery log should be kept wherein the details of the vehicle and its operator are recorded.

10. Finally, management and employees should trust their instincts regarding possible predatory behavior they may observe. If something does not seem right, it probably is not.

EMPLOYEES

1. All employees must have a photo ID on file in the establishment, with a description of his or her position and contact information. Consider using ID scanning not only for patrons (see below) but also for employees. This roster of employees present could be critical in the event of an evacuation or other emergency.

2. Establishments should also have contact information, including social media accounts, for all individuals contracted to provide operational services such as DJ's and promoters.

3. There must always be a person present designated to be in charge of the premises. The name and phone number of both the manager and the person designated to be in charge must be made available to appropriate government agencies.

4. Employees should regularly clean up inside and outside the establishment. All flyers, handbills, cigarette butts, and any other debris, etc. should be cleaned from in front of the premises throughout the night.

5. Designate specific employees to conduct occupancy counts periodically throughout the night.

6. Managers should identify themselves to first responders or other government officials who arrive at the establishment.

7. The New York State Security Guard Act of 1992 mandates the training and registration of security guards. All security guards are required to complete an 8-hour Pre-Assignment Training Course prior to applying to the Department of State for a Security Guard Registration Card, followed by a 16-hour on-the-job training course for security guards within 90 days of initial employment. All security guards must complete an 8-hour annual in-service training course for security guards every year thereafter. Security guards are required to carry their registration card while working.

AGE VERIFICATION

1. State law (Alcoholic Beverage Control Law Section 65-b(2)(b)) specifies the types of documents that are acceptable proof of age for the purpose of purchasing alcohol in New York State. They are: a valid driver's license or non-driver identification card issued by the Commissioner of Motor Vehicles, the Federal Government, a State Government, Commonwealth, Possession or Territory of the United States or a Provincial Government of Canada; or a valid U.S. passport, or valid passport of any other country; or a valid military ID from the U.S.

2. ID should be checked for every person seeking to enter the establishment who reasonably appears to be less than 25 years of age. There should be no exceptions made to this policy, including for anyone brought into the premises by an employee or promoter. Management should monitor the door and make it clear to promoters that they are not to steer patrons around security in order to evade ID checks.

3. The use of ID scanning machines is strongly recommended. While they do not reject legal ID's being used by another individual, nor are they infallible in rejecting fake ID's, they are extremely helpful in recording who is entering the establishment.

4. Some machines are able to both verify that an ID is valid and record who was present in the establishment on a given night. This can be extremely useful in case of an emergency and also to defend false liability claims. Certain machines allow notes to be made about problematic customer behaviors. This may to useful in preventing readmission of the problematic person at a later time.

5. Retain all ID records for a minimum of 14 days. These records must be turned over or made available to the Police Department on request and in some circumstances may be used in defending a charge of serving a minor.

6. Digital video cameras and ID scanners, when used, should be time stamped so that ID scanning information can be compared to video of patrons entering the club.

7. The records created by ID scanning equipment should not be used for marketing or advertising purposes.

PROMOTERS

1. Establishments which contract with promoters may well be held responsible if promoters engage in or encourage irresponsible or illegal activity in the premises. Therefore it is incumbent upon management to take adequate precautions when dealing with promoters, who are much less likely to suffer the consequences of illegal conduct than the establishment itself.

2. Establishments should only work with promoters who are professional. Promoters should be required to provide full contact information for themselves and anyone they hire to work in the establishment. The promoter should be insured, and the venue should be listed as additionally insured on all relevant policies.

3. Management should review the promoter's social media content. Promoters whose social media history indicates problematic conduct should not be used. Additionally, management should require that all promotional materials and social media content concerning the venue be approved prior to being published or released to the public.

4. Management should make absolutely clear to promoters what their policies are, especially regarding admission of those under 21 years old, and make clear that promoters are expected to fully adhere to these policies.

5. Management should have representation at the door to ensure that all door policies are adhered to by promoters and their employees. Management should reserve the right to refuse entrance to any guest pursuant to their existing admission policies.

6. All guests of the promotional team must be treated as any other patron, consistent with the establishment's search and ID policies, without exception, and including the promoters themselves, DJ's and employees.
7. Management should check the past performance of promoters before considering contracting with them, by inquiring with other venues about what type

of clientele they attract, how they operate, how responsive they are to problems or concerns, etc.

CLUB POLICIES

1. Club policies should be clear and well known to employees, patrons, law enforcement, and subcontractors such as promoters and DJ's. It is crucial that club policies are uniformly enforced. For example, if club policy is that everyone entering is first checked with a metal detector, it is important that all persons, including VIP's, subcontractors, invited guests, and entourages be checked. An employee handbook, signs for patrons, and social media postings are effective ways to inform people about club policies.

2. Do not admit anyone under 21, except that those under 21 may be admitted to establishments when operated primarily as restaurants during those hours in which meals are served.

3. It is especially crucial that no one under 21 be admitted in establishments which offer bottle service at tables. It is extremely difficult to monitor patron use of alcohol in a bottle service situation. Overconsumption and underage consumption are all too likely. The establishment is responsible for all alcohol consumption that takes place inside the venue, even if the patrons are doing the pouring. Therefore the safest course of action is to not admit anyone under 21. Even so, establishments must take sufficient steps to ensure that the tables are closely monitored so as to prevent over consumption.

4. A policy handbook should be in the establishment at all times and should be distributed to all employees. The handbook should incorporate the guidelines suggested in this document to the degree practicable. The handbook should inform all employees how to handle situations that arise frequently and which often lead to problems, for example:

    a. illnesses or injuries
    b. fights
    c. patron refuses search or pat down
    d. disorderly patron
    e. false ID
    f. drug use
    g. citizen's arrest
    h. recovered weapon

5. The establishment policy handbook should also include:

    a. emergency plan
    b. counter-terrorism plan
    c. exit plan – gradual staged exit at closing to ensure orderliness

d. plan to maintain order outside the premises
e. club policies

6. Professional signs containing a patron code of conduct should be displayed inside the establishment.

7. When an establishment has residential neighbors, signs should be posted encouraging patrons to be quiet and sensitive to the neighbors at all times. Establishment personnel should be trained to encourage patrons to be considerate of the establishment's neighbors.

8. All permits must be kept up to date and readily available.

9. To ensure that club policies are adhered to, management should implement periodic review of the club policy handbook, training of new employees, refresher training of all employees, and management supervision and instruction.

10. If a criminal incident occurs, an incident report listing full details should be generated and maintained for three years. Attached is a suggested form which may be used for this purpose. Also attached is a set of best practices which has been developed for responding to serious criminal incidents.

POLICE – COMMUNITY RELATIONS

1. A list of all scheduled events should be sent to the community affairs officer and the neighborhood coordination officer (NCO) in the local precinct. In the case of a special event, such as a celebrity performance or party, 72 hours' notice, when possible, should be given to the precinct, and the establishment should ensure that adequate and additional security personnel are employed to meet the expected crowd.

2. Each establishment should have a search policy and adhere to it. (This may vary from no one is searched, to all bags are searched, to random searches are conducted, to everyone is searched.) This ensures that upon arrival, all police officers will have a basis to know if the occupants have been searched and what, if anything was found.

3. Representatives of establishments are welcome at Precinct Community Council meetings, and should attend as many as possible.

4. The Precinct Commander and establishment owners should meet as necessary in order to discuss operational issues, solutions to common concerns, problem locations, etc.

SOCIAL MEDIA

1. Since the publication of the 1st edition of this guide, social media has become an important method of communication in our society. It is especially important in the marketing and advertising of the nightlife industry. It has also become an important tool for law enforcement to communicate directly and instantly with the public.

2. Management of the establishment should subscribe to local precinct and other law enforcement social media feeds to ensure that they are informed of local conditions.

3. All social media content by the establishment for marketing and advertising should be consistent with club policies. For example, if people under 21 are not admitted, that should be made clear.

4. The social media accounts of subcontractors (such as DJs and promoters) and groups seeking to hold events in the venue should be reviewed before employment begins and before any event is contracted for. Objectionable social media content by one of these individuals or groups could reflect negatively on the establishment, and may also attract problematic patrons or protestors.

5. Management should closely monitor any mention of the establishment in social media. Negative materials should be addressed. Monitoring social media is also an important component of counterterrorism efforts. See the section entitled "Counterterrorism Best Practices", below.

RESPONSE TO SERIOUS CRIMINAL INCIDENTS – THE CRIME SCENE

These best practices are designed to apply to serious criminal incidents, usually assaults that are physical and/or sexual in nature. For these purposes assaults are deemed serious when the victim of the physical assault is either unconscious, or is in need of immediate medical treatment, for a serious or life-threatening injury, such as a stabbing or slashing. An exception to this general rule is sexual assault crimes where the victim may have no visible injuries. Sexual assaults are serious criminal incidents and as such fall within the purview of these guidelines.

The Crime Scene - Pre-Incident:

1. All establishments should maintain a list of all employees and independent contractors (such as DJ's, promoters, and other entertainers) who are present on any individual night. Also maintained should be contact information for these employees to aid in contacting them as part of a post-incident investigation.

2. Establishments should request and maintain contact information for a representative of any private group who has a function or event at the establishment.

The Crime Scene - Post-Incident:

3. Call 911 immediately.

4. Establishments should make clear to all managers, employees and private contractors that they are required to tell the truth to police investigators, as a condition of their employment.

5. Do not clean up the crime scene. Protect it from any changes. Crime scenes can be protected by temporarily surrounding them with velvet ropes or yellow "caution" tape, using chairs, velvet rope stanchions or even potted plants to support the tape. To this end, inexpensive yellow "Caution Tape" should be kept in the establishment.

6. Nightlife establishment employees should be aware that important physical evidence may not be readily visible or obvious. Incidents involving sexual assaults will rarely have recognizable evidence at the scene of the occurrence. Establishments should therefore "overprotect" the area of the crime by safeguarding an area larger than they initially believe the crime scene to be.

7. Immediately identify and preserve financial transaction information for all parties involved: witnesses, victims, and perpetrators. This information includes debit and credit transactions. If any people involved were seen taking pictures or apparently using social media, this fact should be brought to the attention of the responding police officers.

8. Involved parties or witnesses should be detained if possible. There are several techniques to accomplish this, from asking them to stay, to offering them complimentary admission on a subsequent date, to asking for and retaining their ID's and giving them to the responding police officers.

9. Establishments should know what parking facilities are commonly used by their patrons and provide this information to police investigators.

10. If the perpetrators or witnesses leave, a description of the vehicle in which they left (with license plate number), the direction and means by which they left, and the identity or description of any people they left with should be provided to the responding police officers.

11. The table or area where the involved parties sat or stood, including their beverage glasses, utensils, and any other evidence should be preserved and left untouched inside the club. This material should be identified to the responding

police officers immediately. Employees of nightlife establishments should be cognizant that in certain circumstances, tampering with physical evidence can be a crime. See, for example, Penal Law § 215.35 Tampering with physical evidence; definitions of terms, and Penal Law § 215.40 Tampering with physical evidence.

12. Video of people inside the club during the evening the crime took place should be preserved for the police even if it appears to have no apparent value. Often these videos can be enhanced to reveal important evidence. To increase the usefulness of these images in establishments which are often dark, some areas of the club, such as a hallways immediately outside the rest rooms, should have enhanced lighting. This will make the images of people passing through that area more identifiable. It is recommended that properly working and maintained digital cameras be mounted in front of the establishment (both inside and outside), at all entry doors and outside the bathroom doors. These digital videos should be recorded, maintained, and provided to the responding police investigators. These videos should be accessible at all times. Whenever the establishment is operating, there should be a manager or security staff member present who knows how to operate the system and retrieve videos.

13. ID scanner information should be preserved and made available to the responding police officers.

14. Serious assaults should always be the subject of a uniform incident report being completed by a managerial level employee of the establishment who was present at the time of the incident. This manager need not be a witness to the incident, but is responsible for interviewing the witnesses and completing the report. The report should be maintained by the establishment for a minimum of the three-year statute of limitations for negligence law suits.

15. Obviously, these best practices apply to serious incidents that occur inside the establishments. However, important evidence may exist inside the establishment even if the crime occurs outside the establishment, and therefore there will be circumstances where these best practices apply to incidents that take place outside of the establishment. For example, if the circumstances of an assault are such that the involved parties were in the establishment before the assault, and the assault subsequently took place outside of the establishment, the evidence that the involved parties left behind must be safeguarded. This includes:

    a. Financial records of their purchases
    b. Video images of involved parties
    c. Images of scanned ID's
    d. Glasses and utensils used by the involved parties, which may yield identifying information such as fingerprints and DNA
    e. Observations of witnesses which may aid in a subsequent identification of involved parties

RELEVANT NEW YORK STATE PENAL LAW SECTIONS:

Section 215.35 Tampering with physical evidence; definitions of terms.

1. The following definitions are applicable to section 215.40:
    a. "Physical evidence" means any article, object, document, record or other thing of physical substance which is or is about to be produced or used as evidence in an official proceeding.
    b. "Official proceeding" means any action or proceeding conducted by or before a legally constituted judicial, legislative, administrative or other governmental agency or official, in which evidence may properly be received.

Section 215.40 Tampering with physical evidence.

2. A person is guilty of tampering with physical evidence when:
    a. With intent that it be used or introduced in an official proceeding or a prospective official proceeding, he (a) knowingly makes, devises or prepares false physical evidence, or (b) produces or offers such evidence at such a proceeding knowing it to be false; or
    b. Believing that certain physical evidence is about to be produced or used in an official proceeding or a prospective official proceeding, and intending to prevent such production or use, he suppresses it by any act of concealment, alteration or destruction, or by employing force, intimidation or deception against any person.
    c. Tampering with physical evidence is a class E felony.

COUNTERTERRORISM BEST PRACTICES

1. This section is intended to provide basic information on counterterrorism planning to nightlife businesses. It is not intended to alarm or frighten, but rather to help New York City's vibrant nightlife community achieve both safety and hospitality for its customers.

2. Effective counterterrorism measures can only be achieved through cooperation. To achieve the goal of a safe New York City nightlife, operators of nightlife establishments will have to work cooperatively with the police, nightlife industry associations, their landlords, their neighbors, and even their competitors.

3. The following is a starting point for nightlife businesses to create an effective counterterrorism plan. In creating such a plan, nightlife businesses are encouraged to consult their local police precinct, as well as private security and nightlife management consultants.

Terrorist Strategy

1. Terrorism is a criminal act designed to manipulate an audience beyond the immediate victims. Terrorists seek to commit acts of violence that draw local, national, and international attention to their cause. Terrorists plan their attacks to obtain the greatest publicity and choose targets that symbolize the ideologies they oppose.

2. Terrorists engage in violent behaviors for the following reasons:

    a. To create fear in people they consider enemies.
    b. To create recognition for their ideology.
    c. To provoke a reaction from governments.
    d. To obtain money and equipment from their sympathizers.

3. Terrorist target selection is often based upon the ability to inflict mass casualties, the symbolism of the target, and the vulnerability of the target.

4. Recently, there seems to be a trend to select “soft targets,” those with less security than “hard targets” like government or military facilities.

5. Islamic extremists view nightlife establishments as “dens of depravity,” which represent Western decadence and immorality. Patrons of these businesses are viewed as sinful and deserving of violent punishment.

Examples of Nightlife Attacks

The following are notable examples of terrorist attacks against nightlife establishments:

1. Pulse Nightclub Attack, June 2016, Orlando, Florida

    a. Sunday, June 12, Omar Mir Seddique Mateen opened fire at Pulse, a well-known gay nightclub in Orlando, Florida. 49 killed, 53 wounded

    b. The suspect, Omar Mateen, pledged allegiance to the terrorist leader Abu Bakr al-Baghdadi in a call to 911, during the attack.

2. Paris Attacks (specifically, the Bataclan Concert Hall), November 2015, Paris, France.

    a. On Friday, November 13, a major terrorist operation involving multiple attacks on 7 locations occurred in Paris, France. At least 129 people were killed and 415 were wounded in the attacks.

    b. The deadliest phase of the attack took place at the Bataclan Concert Hall, a performing arts venue that holds approximately 1,500 people. While

initially reported as a hostage situation, it appeared that at least three attackers dressed in black, armed with AK-47 assault rifles, and equipped with suicide vests entered the sold out venue and opened fire on the audience, killing 89.

3. Tiger Tiger Nightclub Attempted Attack London, June 29, 2007, London, England

    a. Two car bombs were discovered and disabled before they could explode.

    b. The first device was set near the Tiger Tiger nightclub at around 01:30 am, and the second was nearby, in an area of London popular for its many nightlife establishments.

    c. Tiger Tiger is the flagship of one of England's best known nightclub chains. It is 18,000 square feet in size, and contains a restaurant, four large dance floors, and five bars.

    d. The first car was reported to the police by an ambulance crew tending to a minor incident at the nightclub. The ambulance crew noticed suspicious fumes coming from the parked car.

    e. About two hours later, the car containing the second device was towed because it was parked illegally. The staff at the auto pound noticed a strong smell of gasoline emanating from the vehicle and reported it to police. The cars, both late model Mercedes, were found to contain improvised explosive devices made up of gasoline, propane gas, nails, and a remote triggering device.

    f. A member of a radical Islamic group was convicted of this attempted attack.

Characteristics of Terrorist Attacks

Terrorist attacks typically involve:

1. Careful planning by the terrorist. These are almost never spontaneous attacks. The planning and rehearsal by the terrorists provide an opportunity to detect and prevent the act.

2. Hostile surveillance. Hostile surveillance is intelligence gathering about the potential target by the terrorists. Active shooters, for example, frequently plan and rehearse their attacks in advance. Terrorists planning an attack may trigger a false alarm to gauge security and first responder response.

3. Hostile surveillance is usually conducted in a covert manner, with the terrorists conducting the surveillance pretending to be tourists, students, or customers. It is

often characterized by activities such as photography, videography, sketching or drawing, and note taking. Often the person or persons conducting the hostile surveillance will take particular interest in the outside of a potential target, paying particular attention to the doors, alarm systems, video surveillance systems, parking lots, security personnel and security plans. Sometimes these individuals may engage employees and ask questions about the establishment's operations and its security plans.

4. Secondary explosions. Secondary explosions are designed to inflict mass casualties and death on victims fleeing the initial attack, and on emergency personnel who respond to the initial incident.

5. Lone Wolves: A lone wolf is someone who commits violent acts in support of a group, movement, or ideology, but who does so alone, outside of any command structure, and without material assistance from any group. Although the lone wolf prepares and acts alone, the perpetrator may be influenced or motivated by the ideology and beliefs of a group. Frequently, a lone wolf becomes "self-radicalized" via social media and the internet.

Counter-Terrorism Security Planning

1. Competent and cost effective security systems involve a combination of security personnel, other non-security establishment employees, and electronic systems such as alarms, video surveillance, and access control. To ensure maximum effectiveness and efficiency, these systems should be designed, managed, and maintained by a professional. Unlike the systems in use 20 or 30 years ago, modern systems are integrated and allow a wide variety of access, management, supervision, review and control. This includes remote access to many features through secure internet connections.

2. Modern security systems are multipurpose. They seek to prevent criminal activity, terrorist attacks, and to ensure a safe environment free of liability on the part of establishment ownership and management.

3. The counterterrorism goal of all security systems is target hardening. That means making the establishment more difficult to target for terrorist attacks. In order to be most effective, these target hardening efforts must be based on current data about recent terrorist activity. It is therefore crucial that the person responsible for security and counterterrorism remains well informed about developments in this area.

4. The goal of a comprehensive security plan is to protect life and property through deterring, detecting, delaying, denying, and responding to threats. The foundation of a suitable protection plan should be an appropriately sized and professionally managed security force. This force should consist of personnel

specifically organized, regularly trained and equipped to protect the facility's assets.

5. A professional security force can serve as an invaluable target hardening asset. The basic functions of the security force should include:
   Controlling entrances and pedestrian movement
   Patrolling the facility's interior and exterior
   Escorting personnel and material
   Inspecting for security and fire exposures
   Monitoring video security and alarm systems
   Responding to emergencies

6. All security personnel are vulnerable to attack due to the nature of their jobs; however, strategically placed security personnel are obstacles that must be avoided, distracted or eliminated in order for a criminal or terrorist to accomplish his or her goal. Failure to provide an adequate security presence reduces the security officer's ability to perform their duties and responsibilities.

7. Each organization that employs security officers should create its own organization-based training program. The training program's objective is to ensure that all personnel are able to perform routine and emergency duties competently and efficiently. Periodic training is an effective means of obtaining and maintaining maximum proficiency of security personnel. A good training program benefits both the organization and the security force. The task of supervising the force is made easier, there is less wasted time, fewer mistakes are made, and there is less friction with non-security personnel. A good training program helps instill confidence through developing increased proficiency. The training establishes systematic and uniform work habits, requiring fewer personnel to accomplish the same goal. Security personnel should receive training in counter-surveillance, criminal and terrorist indicators and behavioral pattern recognition in order to familiarize themselves with the criminal and terrorist mindset. This training curriculum will help ensure that all security personnel become familiar with current tactics, methods of concealment and distraction techniques being utilized by criminals and terrorists worldwide.

8. A resource for current information is the NYPD SHIELD program. NYPD SHIELD is a public-private partnership based on providing best practices, lessons learned, counterterrorism training opportunities, and information sharing. SHIELD seeks to partner with private sector security managers with the goal of protecting New York City from terrorist attacks. More information on NYPD SHIELD, and an application to join, can be obtained from their website, www.nypdshield.org. If you are interested in receiving additional training or have questions about any of these issues, additional resources are available at SHIELD, The NYC Hospitality Alliance, https://www.thenycalliance.org and The Responsible Hospitality Institute, http://rhiweb.org.

9. Responsibility for counterterrorism security planning should be assigned to one senior managerial employee, usually the same person responsible for other types of security. This individual should have sufficient resources and authority to accomplish this responsibility.

10. The establishment should have a counterterrorism security plan. The plan should be simple, clear, and flexible. The plan should consider all aspects of establishment security, both inside and outside of the location. This plan should include:

    a. Details of the steps to be taken if an emergency occurs. This should include the personnel assigned to perform these functions, with designated back-up personnel assignments.

    b. Instructions on how to respond to a threat, such as a bomb threat or threat of attack delivered by telephone or in person

    c. Instructions on how to respond to the discovery of a suspicious device.

11. A search plan. Searches should be conducted daily, before, during and after hours of operation. Search plans should be created in advance and should be memorialized onto a checklist. The checklist should be completed each time the establishment is searched. Searches can be incorporated as part of the routine cleaning and maintenance of the establishment.

    The search should also be performed when accompanying the police in response to a specific threat against an establishment, such as a telephone bomb threat. In these cases it is much more effective to have the responding police officers accompanied by employees who routinely search the establishment. It will be easier for these employees to recognize out of place, unusual, or suspicious items than it would be for police officers who may have never seen the establishment before.

12. An emergency action plan. Create an Emergency Action Plan (EAP) and conduct training exercises practicing the various aspects of the plan. The plan should include shelter in place plans for situations such as active shooter scenarios, and evacuation plans for suspicious package/device scenarios.

13. All establishments should have a written evacuation plan. The evacuation plan must include clear communication to staff and patrons. All routes, exit plans and assembly areas must be well defined. Staff members should be trained to act as marshals (leaders/coordinators) and contacts once the evacuation assembly area is reached.

When designing evacuation plans, it should be noted that secondary explosives are used by terrorists to inflict casualties on people fleeing an initial attack. The evacuation plan should therefore include alternate assembly areas

14. A communications, media, and social media strategy, which includes liaison with the police and other emergency services, communication with the media, and inquiries from concerned family members.

    a. Management should monitor all social media mentions of their establishment. People who intend to attack a target often discuss their grievances toward their potential target in social media or other forums. These threats should be taken seriously and reported to the police. Social media aggregators are useful to monitor multiple platforms.

    b. In a similar vein, attention should be paid to patrons who make threats, have repeated negative interactions with security personnel, or who repeatedly appear at the establishment dressed in pseudo-military clothing. Behaviors such as this should be brought to the attention of management, who will determine if it is serious enough to be reported to the police.

15. An active shooter plan. In the case of an active shooter situation, follow the "ABC's":

    Avoid or evacuate the area. If that is not possible, then
    Barricade yourself in a safe area. If that is not possible, then
    Confront the shooter as a last resort if all other options are exhausted.

    a. In any possible active shooter situation, all non-emergency personnel should be prevented from entering the area. Occupants of the area should be instructed to remain calm, silence their electronic devices, and to follow the instructions of emergency personnel arriving at the location.

    b. The security plan should include the "SEVEN KEY INSTRUCTIONS," which are applicable to most incidents:
        1. Notify the police immediately.
        2. Do not touch any suspicious items.
        3. Evacuate, if possible, to a safe distance. Remain behind hard cover.
        4. Prevent others from approaching any suspicious item or entering the area.
        5. Communicate with staff and patrons in a manner designed not to create alarm.
        6. Do not use radios and cellular phones in the immediate vicinity of any suspicious item. Remain quiet and silence all electronic devices.

7. Ensure that witnesses – whoever found the item or witnessed the incident – remain present to talk to the police.

16. A perimeter security plan. The primary security concern is enhancing the "first line of defense" – the perimeter. The goal of perimeter security is to provide some measure of deterrence, delay, and prevention against hostile acts. This will provide an appropriate level of security with minimal patron interference. The configuration of obstacles that create the protective layers should be a risk-based integration of personnel, equipment, and procedures. These measures should be scalable as threats change, and flexible to avoid predictability.

17. Perimeter security design involves two main elements: 1) the prevention of unauthorized vehicles and pedestrians from entering; 2) access control points at which pedestrians are vetted and screened before allowed entry. Access control is a key component of a facilities security system. The goal of access control is to facilitate access to specific areas for authorized personnel and to deny access for unauthorized personnel.

18. All staff should be trained on the counterterrorism security plan so that they understand their responsibilities, and also have a general understanding of sound counterterrorism practices. Refresher training and training of new employees should be conducted periodically. Constant vigilance is the most important concept to be conveyed to the staff.

19. Training should include when and how to notify the police and senior management. Management should be notified whenever staff notices anything unusual or suspicious. The police should be notified anytime a possible threat exists. Call 911 for emergencies and crimes occurring or about to occur. For example, call 911 if an employee believes the establishment is currently being subject to hostile terrorist surveillance. Call the New York City Terrorism Hot Line at 1-888-NYC-SAFE or 1-888-692-7233 if possible terrorist related activity has occurred in the past. The hotline can also be emailed at NYCSAFE@nypd.org. For example, call or email the hotline if an employee recalls seeing activity in the past that may have been indicative of terrorist hostile surveillance. Call 311 to report other non-emergency and quality of life conditions.

20. Door supervisors are an integral component of the security and counter-terrorism plan. They maintain order at the entrance and verify proper identification, while also conducting initial vetting of all persons attempting to gain entry into the facility.

21. Door Supervisors should:
    a. Pay particular attention to fraudulent and forged identification documents. People using apparently forged ID documents who do not appear to be

underage are very suspicious, and should be immediately brought to the attention of the police.

b. Interact with potential customers in a manner to identify any person who may pose a potential threat of criminal or terrorist behaviors.

c. Be responsible by watching for the signs of hostile surveillance of the establishment. This includes being aware of new people on the streetscape surrounding the establishment. These could include vendors, panhandlers, and loiterers. Any incidents of possible hostile surveillance should be reported to management, who will make a determination whether the incident is serious enough to be reported to the police.

22. All screening of people entering the establishment should take place immediately inside the exterior doors. Body "frisks" or "pat downs" are not recommended, as they are rarely conducted in a manner thorough enough to identify where many weapons are concealed. A metal detector is recommended, along with documented training (and re-training) of both management and security personnel. As a part of the door team, a female security staff member is recommended to search purses, and frisk females who set off the metal detector.

23. An appropriate electronic security system is a key component of counter-terrorism preparedness. An effective electronic security system is an integrated system that encompasses all interior and exterior sensors; video security camera systems for assessing alarm conditions; electronic access control systems; data-transmission media; and reporting systems for monitoring, controlling, and displaying various alarm and system information. These components are ultimately brought into a centralized location for monitoring, generally referred to as a command and control center. The complexity of the system will correspond to the characteristics of the establishment.

24. Detection is achieved through the use of intrusion detection and access control systems, video security systems, and patrols. Delay is achieved through the use of locks, turnstiles, fences, and other physical barriers. Response is triggered through one or more of the detection systems. An access control system integrates barriers and technologies to maximize the probability that intruders will be detected before accomplishing their goal. Once there is knowledge that someone is attempting to gain entry into a protected area, an alarm must be generated. The alarm signal should be transmitted to a location in which the alarm can be assessed. Once the alarm is assessed, the assessor must be able to generate a response from security personnel and/or law enforcement. For an access control system to be deemed effective, the time it takes from alarm generation to response from security and/or law enforcement should be less than the time it will take the terrorist or criminal to complete their activity. Failure of the system can occur when any of the components experience technical malfunction or when security personnel monitoring the security cameras fail to identify persons entering restricted areas.

25. A properly integrated video security system (VSS) provides time-saving and cost-effective means of monitoring a large area. Alarm assessment through the use of a video security system enhances existing security functions by determining the appropriate response to an alarm. Recorded images are also valuable when investigating incidents that may lead to criminal and civil litigation. For surveillance purposes, a properly designed video security system provides a cost-effective supplement to security personnel. VSS systems should be professionally installed and maintained, with employees responsible for their use.

26. VSS images should be constantly monitored and recorded. Recordings should be kept for a minimum of 30 days. The quality of the recordings should be regularly checked, ensuring that the images are clear and that the date and time stamps are accurate. Sufficient staff should be trained on the use of the VSS system to allow it to be continually monitored during an incident. Lighting should be appropriate to ensure good image quality.

Suicide Bombers

1. Counterterrorism security plans should include training for all staff in the detection of possible suicide bombers. There are many factors which may create suspicion of this activity: inappropriate clothing; protrusions from the clothing; concealment of the hands; visible wires or tape; people communicating while trying not to be observed; signs of extreme stress or nervousness; and individuals whose speech includes stuttering, mumbling or chanting, or are hesitant or unresponsive.

2. In counterterrorism planning, it is important to stress the need to be vigilant and observe all people, being careful to not exclude individuals from suspicion because of their appearance. Personnel should be mindful of the increased participation of females in terrorist activity.

3. Vehicle Borne Improvised Explosive Devices (VBIEDs): Terrorists have often employed explosive devices hidden inside cars or other vehicles. Counterterrorism training should stress to all staff that all vehicles are to be scrutinized for irregular operation or suspicious activity, including luxury vehicles, limousines, taxicabs, and vehicles purportedly carrying VIPs.

4. The use of bollards or other physical barriers to vehicles may be considered, but their use must be consistent with local traffic and other City regulations and permit requirements. Suspicious activity or irregular or unusual operation by any vehicle should be reported to the police.

5. Communications: Cellular telephones may not function during an emergency. Larger establishments should consider the use of hand held radios for emergency communications. All establishments should consider the installation of a hard-wired (land-line) pulse dial analog telephone which will function during

power failures. Announcements are often important during emergency situations. The emergency plan should include provision for making announcements inside the establishments. DJ's should not be relied upon to make appropriate announcements.

Counterterrorism Recommendations

1. Learn: Stay informed of world and local events, and any ongoing threats. The NYPD SHIELD web site http://www.nypdshield.org. is a good source of current and reliable counterterrorism information. So are the social media accounts of the NYPD and your local precinct.

2. Communicate and Cooperate: Maintain good lines of communication with the police, industry associations, your landlord, your neighbors, and even your competition. It is in all of our interests to ensure that the nightlife industry continues to provide a safe and fun environment for its customers. Terrorism is a societal problem which no single entity can address alone. To have effective counterterrorism planning, we must all work together, and communicate effectively.

3. Plan: Every business should have counterterrorism and emergency plans. The execution of these plans should be the responsibility of a senior, management level employee. The plans should be written, with specific assignments for staff members, and should include back-up assignments to account for staff absenteeism, days off, and terminations. The plans should also include initial training, periodic retraining, and drills.

4. Be Vigilant: The culture of your organization must be changed to stress vigilance on counterterrorism and safety issues. Cultural change in organizations starts at the top, with owners and senior management. All people involved in your organization must understand the focus that is to be placed on looking for suspicious, criminal, and unsafe activities and reporting them. Your counterterrorism and emergency plans must give specific directions as to when and how to notify the police and establishment management.

5. Become a Hard Target: The goal of a successful counterterrorism plan is to make your establishment a "hard target," one that is not perceived by terrorists as desirable to attack. Many factors lead to becoming a hard target, including: increased security, regular searches, counterterrorism and emergency drills with staff, visible cameras, counterterrorism planning, training of staff, and a culture of vigilance.

Attached to this booklet are four useful documents:

1. NYPD SHIELD Bomb Threat Checklist, which is useful when a bomb threat is received over the telephone.
2. NYPD SHIELD Guidelines for Suspicious Mail or Packages.
3. NYPD SHIELD Criminal Description Form, which is useful whenever a description of any person needs to be recorded.
4. NYPD “If you see something, say something” poster.

BOMB THREAT CHECKLIST

CALL 911 Remain calm and try to keep caller on the line.

EXACT WORDS OF CALLER:

_____
_____
_____
_____
_____

Questions to ask the caller:
When is the bomb going to explode? _____
Where is the bomb right now? _____
What does the bomb look like? _____
What kind of bomb is it? _____
What will cause the bomb to explode? _____
Did you place the bomb? _____ Why? _____
Where are you? _____
What is your name? _____
What organization do you represent? _____

VOICE		MANNER		BACKGROUND NOISE	
Loud	☐	Calm	☐	Street	☐
Soft	☐	Coherent	☐	Bar/Restaurant	☐
Intoxicated	☐	Angry	☐	Factory	☐
High Pitched	☐	Emotional	☐	Subway	☐
Deep	☐	Laughing	☐	Office	☐
Accent	☐	Other	☐	Other	☐

Was caller male or female? _____
Was caller's voice familiar? _____
Did caller read a prepared statement? _____
Was caller well spoken? _____
What was approximate age of caller? _____
Telephone number where call was received? _____
Time call received: _____
Date call received: _____
Your name: _____
Your position: _____
Your telephone number: _____
Your email: _____

NYPD SHIELD

COUNTERING TERRORISM THROUGH INFORMATION SHARING

SUSPICIOUS MAIL OR PACKAGES

- Leave the mail or package where it was found. Do not disturb. Do not try to clean the substance.
- Immediately call ***911***
- Clear the immediate area of all persons and keep others away.
- Cordon off the immediate area.
- Instruct people in the immediate area to wash hands and other exposed skin with soap and water.
- Isolate exposed persons to a designated area away from the substance and await further instruction.
- List the names of the persons in the immediate area of the mail or package.
- Shut down all HVAC (heating, ventilation, air conditioning) systems.
- Document the location of mail or package.

CRIMINAL DESCRIPTION SHEET

Physical Description

SEX _____.

RACE _____..

HEIGHT _____

WEIGHT .

COMPLEXION __.

EYES – COLOR – EYEGLASSES

(ALERT – NORMAL – DROOPY)

_____

VISIBLE SCARS, MARKS, TATTOOS

_____.

AGE _____.

Method of Escape

DIRECTION _____.

LICENSE _____....

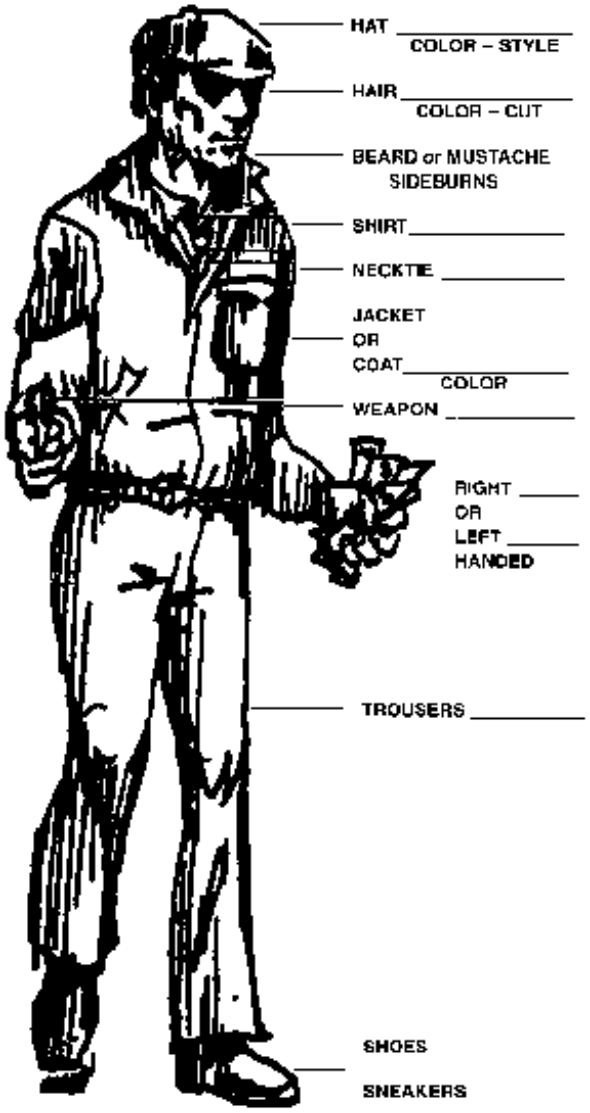
VEHICLE DESCRIOPTION _____...

_____

Remarks _____

_____....

_____.



HELP THE NYPD FIGHT TERRORISM

IF YOU SEE SOMETHING, SAY SOMETHING

TOLL - FREE TERRORISM HOTLINE:

1-888-NYC-SAFE

1-888-692-7233

ALL CALLS WILL BE KEPT CONFIDENTIAL

IN AN EMERGENCY, CALL 911

IN NON - EMERGENCIES, CALL 311