HSEMA's Business Emergency Management Operations Center (DC BEMOC) is dedicated to sharing information and resources that help to protect, prevent and mitigate human-caused threats and hazards in the District of Columbia.

The information in this pamphlet identifies the threats and hazards common to the District and provides potential protective and preventative measures that District businesses can implement to enhance security of their facilities.

These measures are intended to serve as suggestions for possible security improvement. Not all recommendations will apply to you, your facility, and your business's operations.

Become a DC BEMOC member today!
Go to Hsema.dc.gov/dcbemoc to register.

THREATS AND HAZARDS

Knowing which threats and hazards might impact you and your business can help you make the informed decisions regarding your business's security protocols and protective measures.

Consider the following man-made and natural threats and hazards that may occur in the District:

- **Active Shooter**
- **Bomb Threat**
- **Fire**
- **Hazmat Incident**
- **Biological Incident**
- **Civil Unrest**
- **Theft**
- **Transportation Incidents**
- **Flash Flood**
- **Blizzard**
- **Hurricane**
- **Tornado**
- **Hail**
- **Earthquake**
- **Severe Weather**
- **Extreme Heat and Cold**

For more information, contact
DC.Bemoc@dc.gov

BEMOC

READY DC

GOVERNMENT OF THE DISTRICT OF COLUMBIA
MURIEL BOWSER, MAYOR

HOMELAND SECURITY AND EMERGENCY MANAGEMENT AGENCY
DISTRICT OF COLUMBIA
HSEMA

SECURITY GUIDANCE FOR BUSINESS AND COMMERCIAL FACILITIES

PLANNING

- □ Identify critical areas and assets within the facility.
- □ Conduct regular risk assessments and security audits.
- □ Develop a facility security plan, emergency response plan, and business continuity plan.
- □ Designate a POC for facility security, and if appropriate establish a facility security committee.
- □ Conduct regular exercises of plans with facilities, employees, management, tenants, contractors, and customers.
- □ Establish procedures for building evacuation and for shelter-in-place situations.
- □ Conduct regular evacuation drills with facility employees, clearly outlining the evacuation routes and outdoor assembly points.
- □ Develop policies and procedures for dealing with hoaxes and false alarms.
- □ Establish liaison and regular communication with local law enforcement and emergency responders.
- □ Maintain a constant awareness of the current threat condition and available intelligence information.

ACCESS CONTROL

- □ Issue photo identification badges to all employees, contractors, cleaning crews, vendors, or temporary employees. Require the badge be displayed at all times.
- □ Require sign-in/sign-out for visitors. Issue special identification badges to visitors.
- □ Limit access to contractors, vendors, and temporary employees who are expected and whose presence has been confirmed by prior arrangement.
- □ Define and secure controlled areas that require extra security.
- □ Provide appropriate signage and restrict access to non-public areas and secure rooms.
- □ Provide adequate door and window locks and other access controls to areas where access is limited.
- □ Add intrusion detection systems and alarms to doors, windows and other openings. Test detection systems regularly.
- □ Establish a process for controlling access and egress to the facility; including designated, monitored points of entry.
- □ Ensure that illegally parked vehicles are moved or towed.

COMMUNICATIONS

- □ Install, maintain, and regularly test the facility security and emergency communications system.
- □ Develop redundancy in the facility security and emergency communications system.
- □ Develop a notification protocol that outlines who and how building management, tenants, employees, and visitors should be contacted during an emergency.
- □ Maintain contact numbers of employees, contractors, vendors, and suppliers in the event of a security-related incident.
- □ Maintain sign-in sheets of all visitors and their contact information.
- □ Take any threatening or malicious telephone call, fax, or bomb threat seriously.
- □ Encourage employees and the public to report any suspicious activity that may constitute as a threat.

PERSONNEL

- □ Conduct background checks on all employees.
- □ Include security awareness into new employee training programs.
- □ Maintain an appropriately sized, equipped, and trained security force.
- □ Check and maintain training rosters to ensure that personnel have received proper training on security guidelines and specific preplanned emergency response measures.
- □ Provide security information, suspicious activity reporting procedures, and evacuation procedures to vendors, contractors, and visitors.
- □ Require contractors, vendors, and employment agencies to vouch for the background and security of their personnel who will work at the facility.

BARRIERS

- □ Evaluate the need for perimeter barriers (e.g., fences, berms, concrete walls) around the facility.
- □ Provide adequate exterior lighting, including emergency lighting, where appropriate, to help in detecting and deter suspicious or unusual activity.
- □ Provide adequate locks, doors, and other barriers for designated areas (elevators; HVAC system, storage, delivery, and utility areas; mechanical rooms; roof).
- □ Install vehicle barriers (e.g., bollards, fencing) to keep vehicles a safe distance from critical areas.
- □ Inspect barriers routinely for signs of intrusion.

SURVEILLANCE

- □ Install video surveillance equipment (e.g., closed-circuit television [CCTV], lighting).
- □ Add intrusion detection systems and alarms to doors, windows and other openings. Test detection systems regularly.
- □ Monitor all people entering and leaving the facility.
- □ Be aware of all vehicles approaching the facility for signs of threatening behavior.
- □ Regularly inspect trash bins, parking lots, garages, utility closets, storage, areas, mechanical rooms, and HVAC systems for signs of suspicious activity.
- □ Regularly inspect designated secure areas for signs of forced or failed entry.