Security Checklist

Security at water districts and authorities has always been an issue that districts and authorities have addressed for the protection of water supplies and treatment. With incidents of active shooter and violence directed at staff, security is receiving even closer scrutiny. The following checklist of security items has been developed through the process of doing several security assessments over the last three years. The list is not comprehensive, nor does it necessarily address specific security issues at your district or authority. The focus here is on public access to district and authority offices, not to water treatment and transport facilities, which fall under Homeland Security requirements. You can always contact the Fund's Risk Management Consultant or Risk Control Consultant for more specific responses.

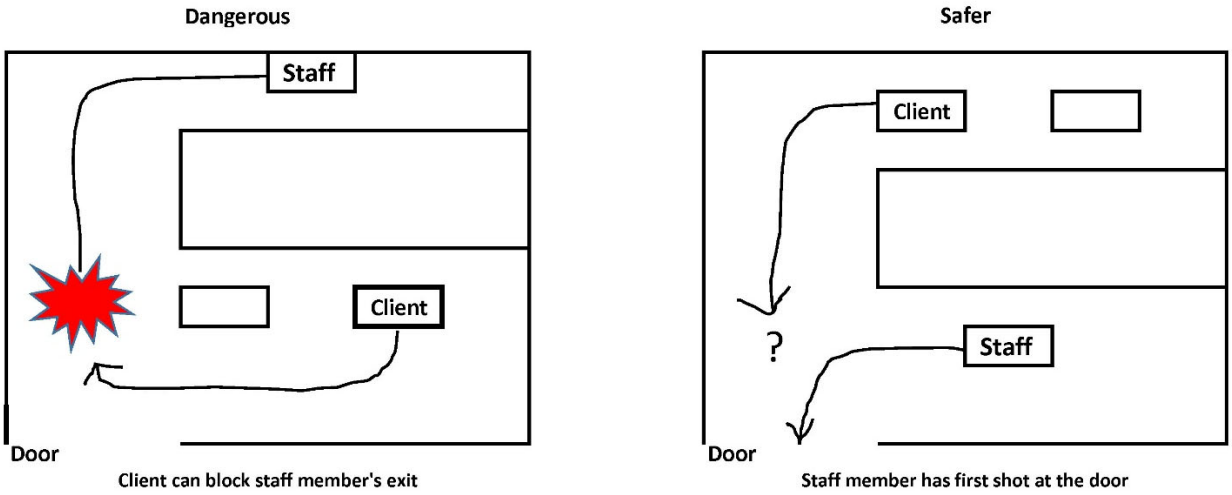
The first section reviews security measures for overall building security.

- Door security is important because most threats to staff and clients enter through the doors. All outside doors, and some internal doors from lobbies to laboratories should have badge or code access. This will prevent most unauthorized access and help the district or authority monitor and control who is actually inside.
- In conjunction with door security is visitor sign-in and badge assignment so that any wandering visitors can be recognized and helped to get where they are supposed to be or escorted out of the building.
- Cameras, both inside and outside, can be effective for monitoring who is outside the district or authority offices and may be in unauthorized places inside. Monitors for the camera system should be visible to on-duty staff so something can be done if there is uncertainty about someone or an act of violence is taking place. Camera feeds that aren't monitored are only good for viewing events after they happen and can't be used for intervention or prevention in real time. All building entries and lobbies should have camera observation. Parking lots and sidewalks should also be covered by cameras.
- Lighting outside the buildings is important for effective camera systems and providing a sense of security for staff arriving or departing when it's dark.
- Vegetation around buildings and parking lots can provide places of concealment and endanger staff, customers, and other visitors entering the district or authority offices. Especially at night, any staff members who are uncomfortable leaving the building should be accompanied as they walk to their vehicles to leave during winter months as it gets dark earlier.

The second section provides a checklist of internal security recommendations.

- Entrapment potential in an office almost killed a psychiatrist last fall at a mental health clinic. His office was set up so the client was between the clinician and the office door.

The shooter was so shocked after he fired at the psychiatrist that he remained seated as the psychiatrist rushed past him to the door. Any district or authority offices where customers with complaints or staff facing discipline or terminations are seen should be set up so the staff member has an unimpeded path to the door (see diagram). Personal preference or where computer or phone cables run can literally get someone killed or severely injured. If office rearrangement is not feasible, staff members should use a conference room or other place where entrapment potential is reduced.



- Glass partitions at reception in lobbies or service desks provide protection for first point of contact staff who welcome customers and visitors. The flimsy plexiglass partitions that became commonplace during the pandemic do not protect staff from angry or violent customers. Glass partitions should be well designed, strong, and capable of providing easy and clear communication through the partition.
- Lobbies should have staff response plans for lobby disturbances and interventions.
- Panic buttons for reception staff, isolated workers, and some offices are an effective alert signal.
- Buzz-in capability for lobby doors into office areas should be installed if card or keypad access is not in place.
- Security associates or guards can be effective if they are well trained and supervised. Develop a posting and responsibilities plan for their use and negotiate your expectations with the security service.
- Action codes for emergency response should effectively alert your staff in the event of an emergency. Resist the urge to have many different codes for any emergency to avoid confusion and prevent delay in response.
- Make sure you have the ability to alert every area in a building.
- An effective response to active shooter events requires planning, preparation, and drills.
- Incident reporting and tracking of security events will help staff allocate security resources, anticipate security events, and prevent them.

Cyber-crime is a violation of district or authority security that can have disastrous consequences and endanger the health and safety of water customers and staff. Your IT departments and senior management should endorse and implement a full suite of protective and preventive measures.

All the measures cited in this article are in place at districts and authorities in Texas. Each district and authority have its own needs and resources to address security. If you need help, please contact the Risk Management Consultant or your Risk Control Consultant for assistance.