Washington State Department of Social & Health Services

Transforming lives

Administrative Policy No. 9.12

Subject:	DSHS Workplace Physical Security Program
Information Contact:	Enterprise Risk Management Office (360) 902-7726
Authorizing Sources:	RCW 9.41.270, *Weapons Apparently Capable of Producing Bodily Harm – Unlawful Carrying or Handling* RCW 49.17.060, *Employer – General Safety Standard* WAC 296-800-100, *Employer Responsibilities: Safe Workplace*
Effective Date:	January 1, 2011
Revised:	July 1, 2016
Approved By:	Original signed by Dana Phelps Acting Assistant Secretary, Services & Enterprise Support

Purpose

This policy requires all Department of Social Health Services (DSHS) appointing authorities to implement and maintain a Workplace Physical Security Program at all locations for which they are responsible. The intent of the Workplace Physical Security Program is to promote an environment where staff, clients and DSHS partners can conduct business free of threats, harm, violence, or intimidation, and be prepared for an active threat situation.

Scope

This policy applies to all DSHS programs and employees, at all DSHS locations.

Additional Guidance

For related, useful information see:

- DSHS Administrative Policy 5.08, *Minimum Physical Security Standards*
- DSHS Administrative Policy 9.01, *Incident Reporting*
- DSHS Administrative Policy 9.11, *Emergency Management*
- DSHS Administrative Policy 14.15, *Building Management of DSHS Leased Facilities*
- DSHS Administrative Policy 15.10, *Information and Technology Security*

- DSHS Administrative Policy 18.62, *Allegations of Employee Criminal Activity*
- DSHS Administrative Policy 18.66, *Discrimination and Harassment Prevention*
- DSHS Administrative Policy 18.67, *Domestic Violence and the Workplace*
- DSHS Administrative Policy 18.76, *Weapons*
- Department of Homeland Security, ***Active Shooter Response Booklet***
- Department of Homeland Security, ***Homeland Security Bomb Threat Worksheet***
- Department of Homeland Security, ***Run, Hide, Fight***

Definitions

Active Threat: One or more individuals actively engaged in killing or attempting to kill persons in a confined, populated area utilizing deadly weapons such as firearms, knives, vehicles or bombs. In these cases there is typically no apparent pattern or method to the selection of victims and any person in the immediate vicinity could be targeted.

Bomb Threat: Verbal or written notification by known or unknown persons of an intention to detonate an explosive or incendiary device, whether or not such a device actually exists.

Client: Any person utilizing the services or benefits offered by a DSHS program.

Client Service Area: Spaces at a DSHS location dedicated to the direct delivery of services or benefits to DSHS clients. This includes such areas as: reception desks, interview cubicles, consultation rooms, etc.

Concealment: The act of hiding at a location which merely blocks you from an intruder's view but offers no benefit of physical protection from a weapon.

Contractor: A company, firm, group or individual operating under a mutually agreed upon, binding, formal agreement with DSHS to provide some specific work, material or service.

Cover: The act of hiding at a location that not only blocks a person from view but has the added benefit of offering physical protection from an intruder's weapons.

DSHS Security Manager: Staff position managed within the Enterprise Risk Management Office that is responsible for the policies, plans and procedures related to the physical safeguarding of Department personnel, financial resources, and capital assets.

Employee: All categories of paid and unpaid full-time, part-time, permanent, and non-permanent workers, volunteers, work-study students, or interns assigned to the Department.

Employee-only Access Area: Designated spaces at a DSHS worksite that are reserved for Department employees to conduct their required positional duties free of general interruption and where movement by the public is restricted. An employee-only access area is typically identified to help ensure the safeguarding of confidential, sensitive and private client information from inadvertent disclosure to unauthorized personnel and to improve employee safety and security.

Employee Identification Card: Visible badge worn by Department staff to indicate their employment with DSHS and typically used to grant them access to restricted areas.

Enhanced Lockdown: Improvised, additional lockdown efforts, such as barricading doors, undertaken by individuals unable to safely egress from the vicinity of an active threat or other potentially violent situation. These efforts are typically used conjointly with traditional lockdown, concealment and cover procedures in order to prevent access and detection by an intruder.

Fight/Confront: The act of physically attacking a violent intruder by using whatever force is necessary to disarm or disable them in an effort to prevent mortal harm to oneself or others.

Hide/Shelter: The process of using enhanced lockdown and other procedures during an active threat situation to prevent an intruder from seeing, hearing or targeting employees.

Hostage: Person who is held captive by a second person, either physically or under the threat of serious physical harm, until such time when the second person's specific demands are met.

Law Enforcement: The generic name for local, state, and federal agency personnel commissioned to protect citizens, maintain law and public order, enforce criminal statutes, and apprehend criminals.

Lead DSHS Program or Lead Program: The DSHS administration that has the greatest employee presence at a given worksite location; the program having the greatest number of staff assigned at a specific business address.

Lockdown: A pre-established response plan intended to be put into effect whenever there is a perceived or actual intruder threat that requires staff and infrastructure, internally and externally, to be secured while the threat is addressed by law enforcement.

Modified Lockdown: A pre-established response plan intended to be put into effect when there is a perceived or actual threat to a location requiring exterior doors to be locked and secured, but allowing normal business operations to continue inside relatively unhindered.

Partner: A representative of another agency, board, commission, or organization collocated or working collaboratively with DSHS for some specific activity, event or project.

Public: The general members of the greater surrounding community or population at large.

Public Access Area: The spaces at a DSHS location designated as unrestricted to the public, including such areas as foyers, hallways, and lobbies.

Restricted Access Area: Designated spaces at DSHS locations with admittance limited to selected employees by virtue of their official duties and responsibilities. These might include

such areas as IT equipment storerooms, inventory storerooms, record storerooms, and negotiable material handling rooms.

Run/Evacuate: A response to an active threat where employees and clients quickly flee the area of the threat to significantly decrease the chance of injury or death.

Run, Hide, Fight: The nationally and generally accepted best response to an active threat. The approach focuses on a series of tiered responses, preferring that people should elect to distance themselves from an active threat (run) whenever possible as the first priority. Second choice would be to use cover and concealment (hiding) whenever running would not be feasible. Lastly, people may choose to confront (fight) an active threat, but should only do so as a last resort when no other options are available. Pre-planning is a major part of the run-hide-fight process, and it is recommended that employees, no matter where they are, consider how they reasonably expect to respond to an active threat in their immediate vicinity if it were to become necessary.

Shelter: Any area at a DSHS location where employees might find protection from some external physical threat, including an active threat.

Suspicious Package: An item or object deemed out of place/context, that cannot be reasonably accounted for, or that is otherwise suspected of potentially being an explosive device or other article intended to cause harm.

Suspicious Person: A person who exhibits out of the ordinary, unusual, or questionable behavior, or is in an area doing something that is not normal.

Tailgating/Piggy Backing: Incidents where unauthorized persons gain access into employee-only or restricted access areas by following authorized staff through employee-only access points and without being challenged by staff for identification.

Threaten: To express (orally, in writing or by action) a direct or veiled intention to do harm, cause trouble, or cause inconvenience to another person.

Victim: A person physically, or psychologically, harmed, injured, or killed as a result of a crime, accident, or other event or action.

Violence: The use of force to physically or psychologically harm another person.

Policy

A. The Department must ensure a safe, secure, professional environment for every employee, client, contractor, vendor, and partner.

B. A Physical Security Survey and Vulnerability Assessment must be performed annually at each DSHS worksite.

C. A location unique Worksite Physical Security Plan must be created, trained to, and

maintained by each DSHS worksite.

D. All employees must read and be trained to the Worksite Physical Security Plan for their specific location.

E. All employees must take part in all local training and drills focused on active threats in the workplace

Procedures

A. Assistant Secretaries/Senior Directors must ensure that a Workplace Physical Security Program is implemented and practiced throughout their program.

B. Appointing Authorities must:

1. Oversee the implementation and maintenance of a Worksite Physical Security Program at each location where their office is the lead DSHS program or the only DSHS presence. They must:
    a. Collaborate with all other DSHS programs and where feasible other state and federal agencies co-located at the site, if any, to determine any special needs, establish methods of communication, and develop a common course of action for emergency events.
    b. Interface with other partners co-located at the site to ensure a common, supportive course of action and establish clear methods of communication when an emergency might occur.
    c. Provide annual training, exercises, or drills focused on physical security in the workplace, including active threat.

2. Implement requirements for the use of some method of standard employee identification by all employees, such as an Employee Identification Card, that also includes progressive discipline and corrective action plans for employees failing to follow established identification procedures.

3. Direct all local managers/supervisors to actively participate in the development, maintenance and ongoing support of their locations Worksite Physical Security Plan. This is particularly critical for managers and supervisors located at sites in which they are not the lead program.

4. Coordinate with the DSHS Security Manager to ensure a physical security survey and vulnerability assessment is conducted at each DSHS worksite annually. Managers are responsible for determining the most appropriate style/extent of assessment to be conducted that best suits local needs and available resources. An example of one possible assessment is available at the following link:

Physical Security Survey and Vulnerability Assessment

5. Ensure a Worksite Physical Plan has been implemented at every worksite for which you have employees assigned. Note that these Worksite Physical Security Plan requirements may be incorporated into other existing written emergency management plans, but should in every case minimally address the following:
    a. A description or diagram of the worksite that clearly identifies:
        1. Public access and client service areas, including primary entrances and emergency exits;
        2. Employee-only access areas, including primary entrances and emergency exits;
        3. Restricted access areas, including primary entrances and emergency exits; and
        4. All available routes of egress.
    b. The local process used to grant and enable entry to the various location spaces, including: public and client service areas; employee-only access areas; and restricted access areas that shall include guidance on methods to prevent tailgating/piggy backing and requirements for identification to be visible at all times.
    c. The recommended action to be taken by employees if a physical security request, event or emergency occurs at the worksite. Specific topics that might be addressed, include:
        1. An employee requests security escort to or from their vehicle;
        2. An employee discloses the existence of a restraining or similar order issued by a court that could potentially impact the workplace;
        3. There is evidence of a break-in or vandalism to the worksite;
        4. The location receives, or is otherwise impacted by, a bomb or other threat;
        5. A client, staff, or other party threatens violence at the worksite;
        6. A client, staff or other party attempts or causes violence at the worksite;
        7. There is an observed or reported civil disturbance near, at, or in the vicinity of the worksite;
        8. There is an observed, or reported, hostage situation;
        9. There is an observed or reported active threat incident near, at or in the vicinity of the workplace; or
        10. An active threat occurs requiring the implementation of Run, Hide, Fight actions in the workplace.
    d. A current telephone list of all local, regional and Department emergency and key contacts for security support and reporting purposes.
    e. Directions to all points of egress and develop evacuation procedures for employees directly exposed to the public, such as: lobby navigators, front desk personnel, field workers, and those who individually council clients or work in client service areas.
    f. The implementation of an employee warning system that utilizes plain language to notify staff and clients of an emergency or active threat situation. This system should avoid the use of code or duress words.
    g. Guidance on the use, display, and maintenance of employee identification, to include, but not be limited to: requiring that identification is visible whenever employees are in employee only or restricted access areas; the need for employees using scan badges to scan the badge each time they enter a controlled area;

employees notify supervisors immediately regarding lost or forgotten badges; and the requirement to escort all non-employee guests when in employee only areas.

One example of a possible stand-alone Worksite Physical Security Plan can be found at the following link:

Worksite Security Plan Template

6. Be certain the Worksite Physical Security Plan accounts for the unique and special needs of every employee, particularly those who require special accommodation during emergency events.

7. Ensure all employees read and understand the Worksite Physical Security Plan.
    a. Make certain all employees receive training on the location's initial Worksite Physical Security Plan and all future revisions of the plan;
    b. Provide all new employees training on the Worksite's Physical Security Plan within thirty days of hire;
    c. Ensure all employees review the most current Worksite Physical Security Plan no less than annually; and
    d. Require employees to participate in annual worksite physical security training, exercises, or drills.

C. DSHS Employees must:

1. Read the location's Worksite Physical Security Plan and indicate their understanding of the plan as established by their appointing authorities.

2. Participate in all local annual training, exercises, and drills testing the Worksite Physical Security Plan and employee's responses to an active threat scenario.

3. Provide feedback to managers / supervisors regarding issues or concerns related to the worksite's physical security.

4. Practice routine situational awareness while on the job. Visualize personal safety practices based on daily routine, work station location, and office layout that best prepares you to respond to all threats or emergencies.