Sample Model Security Management Plan

Element #1: Policy Statement

(Security Management is an important enough topic that developing a policy statement, and publishing it with the program, is a critical consideration. The policy statement can be extracted and included in such documents as a new-hire employment packet, employee handbook, or placed on the company's intranet site.)

A policy statement, in part, might read as follows:

"We are committed to maintaining the security and well-being of our employees, visitors, and the surrounding community. Our security management program is but one aspect of our overall workplace safety efforts. Together, these efforts span personnel, information, and asset security and include training and education activities to help ensure our programs' success. Additionally we will diligently work to comply with all applicable laws, regulations, and standards.

Responsibility for this program has been vested with each department manager. Your cooperation with their efforts will help us all maintain a program that accomplishes all of its goals.

We take specific actions toward identifying security-related threats, including workplace violence, and threats that may exist from domestic or foreign terrorism. You (employees) can expand these efforts by reporting concerns and any security breaches immediately.

Your on-going knowledge and cooperation as well as participation with the Security Programs' efforts will be appreciated, and again, help ensure its success.

Thank You,

Signed by Company Official

Element #2: Compliance with Applicable Laws, Regulations, and Standards

(Comment: To the extent that laws and regulations exist, efforts to comply and how you will comply should be delineated within the plan. All of the compliance efforts may not need to be repeated, specifically within an employee handbook, but should be a tactical element of a program.

Some jurisdictions have not mandated specific plans, but have elements of applicable OSHA regulations, such as the General Duty Clause. In that case, indicate those that do apply. In this example, we'll use a California-based company.)

There are various laws, regulations, and standards that apply to our program. We will comply with, at a minimum:

- Cal/OSHA General Duty Clause T8CCR Section 3203
- Cal/OSHA Emergency Action Plans T8CCR Section 3220
- Cal/OSHA's Guidelines regarding Workplace Security

As other laws or regulations are introduced, we will integrate their provisions into our program.

Element #3: Definitions

(Comment: List definitions in this section that explain certain terminologies not readily understood by all. The inclusion of definitions will help those that have to read and deploy the program and assist in training efforts. Examples of terms that may need definition include:)

- Access
- Bomb threats
- Cal/OSHA
- Education
- Emergency Operations Center
- Incident Reporting
- Response Protocols
- Terrorism
- Threats
- Training
- Workplace Violence
- Others: (fill-in)

Definitions critical to any Security Management Program will be included as they are learned.

Element #4: Management Commitment and Responsibilities

(Comments: Delineate, either in narrative or in outline form, the responsibilities of Senior Management, management, and supervision if their responsibilities differ. These responsibilities can be preceded, if necessary, by an internal use management commitment statement, if desired.)

Management commitment and responsibilities include:

- Program management
- Program review and updates
- Development of a review panel or task force if hazards are identified, or for deployment after an event to assist in its review
- Assisting with training
- Enforcing disciplinary actions as needed
- Interaction and assistance with regulatory and response agencies

This section can also include responsibilities for employees, especially those occupying specific roles (by position, not name).

Element #5: Threat Assessment and Analysis

(Comment: A core element of a Security Management Program is the identification of internal and external threats. The mechanisms for identifying threats can be delineated in this section, detailing when assessments will be conducted, who will conduct assessments, and how findings will be modified at future dates if need be.)

Security threat assessments will be:

- Completed prior to the initiation of this program
- Will be conducted as we become aware of new or potential threats
- Conducted for special events that we are either sponsoring or attending

Our Security Management Committee, under the direction of the (General Manager) will conduct threat assessments on a scheduled or as required basis. In addition, the Committee will provide assistance. The use of other internal or external resources might be necessary as well.

Threats will be qualified utilizing a threat matrix, or other tool that compares operations to threats, and their likelihood and severity. Where possible, mitigating actions and recommendations will be initiated.

The threat matrix, after its initial completion and after any updates or modification, will be submitted to senior management for review and approval.

Element #6: The Role of the Security Program Manager

(Comments: Remember, even though the term security is being used, and this program should be integrated with overall workplace safety activities, an organization may have an existing Security Department. As such alternate terminology may be needed if the two programs remain distinct and report to different managers.)

The role of the security manager includes:

- Lead role in threat assessments
- Program maintenance and updates
- Incident response and coordination
- Chair of the Security Program Committee
- Training Responsibilities
- Coordination with other Departments
- Coordination with agencies and response units

Element #7: Employee Education and Training

(Comments: Distinguish general awareness/educational from the tactical duties or training activities that are required.)

Our program will cover:

- Employee duties and responsibilities
- Event-specific responsibilities
- Threat or event reporting
- Back-to-work/check-in requirements
- Potential disciplinary actions
- Dealing with the media, regulatory agencies, or other entities outside the company

Element #8: Management and Supervisor Education and Training

(Comments: Managers and Supervisors will likely have specific duties and expectations ranging from threat identification and mitigation to their role in event response. Some of the responsibilities may mirror those of the employees, but are likely more specific in event response scenarios.)

For Managers and Supervisors, our program focuses upon:

- Individual or Department duties
- Knowledge and deployment of response protocols
- Assuring employee and other constituent welfare
- Threat or event reporting
- Back-to-work/check-in requirements
- Potential disciplinary actions
- Dealing with the media, regulatory agencies, or other entities outside the company

Element #9: Program Exercises and Drills

(Comments: The training and education activities that will be undertaken for the purposes of the Security Management Program, shall be one of the following: case studies, table top exercises, or small and/or large scale exercises.

The appropriate methodology for training and education shall be at the discretion of the Program Manager.

Case Studies

Case studies are in essence, “paper and pen” exercises. They provide an excellent opportunity to educate employees about the program, their responsibilities and basic response protocols. It is assumed that most case studies are conducted in a classroom setting, but in some instances, “homework” may be appropriate. In such cases, it is essential to have follow-up discussions to determine that the case study participant clearly understood what was being discussed in the assigned materials.

The goal of case studies is to ensure knowledge of plans, procedures and job functions related to threat management, response and administrative activities that may be assigned.

Other case study dynamics include:

- They must represent real world scenarios, and
- Case studies are ideally suited for initial program education as well as that which is specific to a department or specific scenario.

Case Studies will be the primary educational activity for most of the employees. Where necessary or required, training sessions will be provided as well. Case study sessions will, at a minimum, include the procedures to follow in the event of:

(All employees will participate in Case Studies)

- A bomb threat
- A violence in the workplace situation – potential or actual
- Domestic violence occurring within our facilities
- General evacuation requirements due to a technical, human or natural threat
- Others as may be determined by the General Manager or Security Management Committee, as examples.

Case studies will be a required element of initial training for new employees and will occur on an annual basis for all employees at a minimum.

Table Top Exercises

Tabletop exercises expand the scenarios and number of participants to usually include multiple departments, however, Tabletop exercises may be conducted to test only one department’s capabilities.

As such, tabletop exercises are more rigorous and complex than case studies. In addition, tabletop exercises are sound vehicles to ascertain that threat management and response duties are understood and can be implemented.

The goals of tabletop exercises are to validate response and event management capabilities and to test specific protocols, under simulated event conditions.

Review sessions will be conducted at the conclusion of Tabletop exercises, chaired by the Security Manager. Such sessions shall review the successes of the exercise, areas requiring improvement and necessary program modifications.

The results of the exercise shall be summarized and submitted to the management team.

Tabletop exercises will be used for several purposes, primarily as expanded education and training tools for Supervisor's and those who may have responsibilities to help manage an event or is responsible for event communications. In addition to the scenarios highlighted in Case Studies, others that will be included Tabletop exercises at a minimum will include:

(Supervisors and Lead personnel will participate in Tabletop exercises)

- Large-scale natural event, e.g. an Earthquake
- Employee assault with a weapon
- Terrorism, including bio-terrorism

Tabletop exercises will be conducted quarterly at the direction of the General Manager.

Small Scale Drills

Small-scale drills may also be referred to as "functional drills". Small-scale drills are those intended to test the interaction of multiple departments and may involve outside agencies or mutual aid partners.

Activation of the Emergency Operations Center (EOC) is recommended during the course of small-scale exercises. Small-scale exercises are designed to test and validate established response plans and capabilities. In addition, such exercises test the availability of resources and materials in the time of need, including, for example, communications equipment and first aid supplies.

Small-scale drills are scenario based as opposed to general in nature. Thus, based on need, multiple drills may be conducted in any given time period, or may be instituted to test a new procedure or response protocols.

Subsequent to small-scale drills, a review session will be conducted to analyze response dynamics, drill success and areas that need improvement. Findings and documentation of the drill will be provided to the Security Program Management Committee.

Small-scale exercises may require the participation of some Supervisors, and will require the participation of most Management personnel. This is due to the more aggressive nature of the exercise and decision-making elements. In addition to the scenarios outlined in the Case Studies and Tabletop Exercises, the following potential events, at a minimum, will be included in small-scale exercise planning and activities:

(Supervisors and Managers will participate in Small-scale exercises)

- Regional natural event, such as an earthquake
- Intruder with weapon
- Bio-terrorism event
- Political activist
- Regional or facility-specific power failure

Small-scale exercises will be held as required or as situations mandate such exercises, however, our plan calls for two, small –scale exercises per year at a minimum.

Large Scale Drills

Large-scale exercises, or drills, are designed to test the entire capability of the Security Management Program. This includes, reporting, event communications, managing events, utilization of the EOC, interaction with outside agencies and mutual aid partners as well as ensuring that vendors and suppliers can meet their responsibilities at the time of an event.

(Note: At no time should large (or any) scale exercises be conducted where the health and safety of personnel, the community – at-large and guests/visitors to operations may be at risk. Safety must be considered at all times during the planning and conduct of such activities.)

Large-scale exercises are more complex to produce, as they require considerable planning and resource requirements. Wherever possible (and safe), actual operational disruption, to simulate an event should be made part of the exercise.

In large-scale exercises, the EOC, or similar management location and structure shall be activated.

Large-scale exercises, at a minimum shall test the following program elements:

1. Event recognition
2. Communications – the equipment and messages
3. Employee, supervisory and management response
4. Compliance with established protocols
5. Utilization of Security Management plans
6. Utilization of resources established to assist us recognize, respond and recover from an event
7. Utilization of other resources
8. Communication with Mutual Aid partners
9. Activation and utilization of the EOC
10. Communication and coordination with essential vendors and suppliers

During the course of large-scale exercises, the following is recommended:

1. Observers from selected sources be involved as outside exercise reviewers
2. Implement multiple scenario planning. That is, the exercise should recognize the dynamic nature of emergency events, and that rarely, if ever, a single event is resolved without other sub-events occurring which require management.

Large-scale exercises shall be conducted no less often than annually.

Findings of the exercise shall be summarized and submitted to the management team for review and comment.

Note: Large-scale exercises may include any of the threats noted in the Case Studies, Tabletop and/or small-scale discussions. Large-scale exercises will include employees, Lead and Supervisory personnel, management, and senior management representatives. Scenario planning will be the responsibility of the General Manager and Security Manager.

It is our intent to hold one Large –scale exercise per year at a minimum. More may be required due to event development or specific hazard concerns, such as adverse weather patterns or terrorist threats.

Element #10: Specific Program Considerations

Our Security Management Program includes specific considerations for:

- Identification Systems
- Facility Access
- Access Controls

(Comments: Insert into this section your Company's requirements for identifying personnel, vendors, and guests. This section will also include requirements for facility access and the controls that have been implemented. No codes, passwords, or other descriptors should be included that could be used to compromise security-related systems.)

Element #11: Threat Mitigation, Control and Response

(Comments: As threats are identified, every effort shall be made to eliminate, mitigate, or control them.)

This section of our program describes responsibilities for:

- Mitigating and controlling threats
- Specific responsibilities
- Confirming and documenting control efforts
- The Human Resources Department role in threat mitigation, especially regarding threats emanating from or directed towards personnel.

Threat response, other than has specifically been delineated, includes the following:

- Safety first- our goal is to assume the safety of employees as well as all of our constituents. Any actions taken to respond to a threat must be taken with safety as our first goal. If questions arise regarding to safety and health they must immediately be directed to the Security Program Manager.

Element #12: Incident Review and Analysis

(Comments: All incidents and responses will be viewed by the management team and where necessary other internal representatives.)

This section describes our:

- Forms to be utilized during the review process
- The process for review and analysis
- Requirements for documentation, and
- Process to ensure program updates and enhancements are appropriately integrated

Element #13: Specific Response Protocols

Where general response protocols will not suffice for particular threats, the following specific response protocols apply:

- Bomb threats
- Terrorism
- Workplace violence

(Comment: You will have to decide within your company which specific threats may need their own protocols- here are some examples.)

Element #14: Mutual Aid

(Comment: Where mutual aid agreements are critical to the success of your program, they should be made part of your plan.)

Our mutual aid agreements extend to:

- (Business Partners)
- (Possibly municipal relationships)
- (Contractually obligated organizations)
- (Recovery partners)

(It is essential to include within your plan how to get in touch with all of the mutual aid partners and what their specific role and/or obligations are.)

Element #15: Communications

(Comments: This section is intended to describe, or list, communication tactics, options, equipment, etc., including those that may be included in the Emergency Operations Center.)

Element #16: Programs Included by Reference

(Comments: Include in this section, other programs that apply that you feel need to be incorporated. The best example might be your Workplace Safety Program, or perhaps, certain aspects of it, where specific safety and health measures may apply for those responsible for responding to events. Your emergency response program should be incorporated as well.)

Element #17: Appendices

The following items are included as critical elements within the Security Management Program:

- Training outlines and documentation
- Call-out lists- numbers and alternates
- Mutual aid agreements
- Maps
- Blueprints, floor plans, evacuation maps
- Area map
- Government agency (FBI, Police, Fire, etc.) contact information