OCTOBER 2001

Site Security Guidelines for the U.S. Chemical Industry

A PRODUCT OF PARTNERSHIP AMONG

AMERICAN CHEMISTRY COUNCIL
CHLORINE INSTITUTE, INC.
SYNTHETIC ORGANIC CHEMICAL MANUFACTURERS ASSOCIATION

This document was produced by Hallcrest Systems, Inc. Hallcrest staff wish to thank American Chemistry Council staff members Kari Barrett and Christina McWilson for their project coordination and support. Also, we appreciate the assistance of Dr. Robert Smerko of The Chlorine Institute, Inc. and Angela DeConti, James Cooper, and Eric Clark of the Synthetic Organic Chemical Manufacturers Association.

Finally, we are grateful to all the members of the ACC Site Security Subgroup and the chemical industry experts at the Security Roundtable meetings for their insights and helpful suggestions.

Contents

Section 1: Introduction

Attention to security is a natural corollary to the chemical industry's safety culture. By reducing the risk of a wide range of threats and mitigating the effects of such incidents as vandalism, sabotage, workplace violence, and even terrorism, security measures can serve the goals of process safety management, risk management, and Responsible Care®. Security efforts, like safety efforts, protect the community and company employees while keeping a chemical plant operational and profitable.

In this era of heightened concern about terrorism, sabotage, and industrial espionage, managers at chemical facilities may have even more reason to attend to the security of their companies' people, property, and information. Building on "Management Practice 15: Site Security" in the Responsible Care® Employee Health and Safety Code, this guide outlines elements of security programs and suggests security practices that managers can consider and tailor to their facilities' particular situations. It provides options and examples, presents sample policy statements and identifies resources for further assistance.

This guide was developed by the security consulting firm Hallcrest Systems with guidance and input from the American Chemistry Council Site Security Subgroup, the Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc.. The suggestions it contains were informed further by the findings of a survey of current security practices at U.S. chemical facilities. This guide is a tool, not a standard.

A. Audience and Objectives

This guide is written for plant managers, operations managers, and other managers with responsibility for security at their sites. The guide's purpose is to help managers better protect employees, the community, the environment, plant operations, and company information and product.

B. Scope

This guide addresses security at fixed facilities and is intended to be a resource to help managers at individual facilities make decisions on appropriate security measures based on risk. The guide does not attempt to provide an all-inclusive list of security considerations for chemical companies, nor does it address transportation security.

In general, a security management effort, could, according to the company's needs, consist of the following elements:

- Risk assessment and prevention strategies
- Security policies
- Collaboration with other corporate departments and with local, state, and national law enforcement agencies, local emergency planning committees, etc.
- Incident reporting systems
- Employee training and security awareness
- Incident investigations
- Emergency response and crisis management
- Periodic reassessment of the security plan for physical security, including access control, perimeter protection, intrusion detection, security officers, ongoing testing and maintenance, and backup systems
- Employee security measures (including prudent hiring and termination practices)
- Workplace violence prevention and response
- Information, computer, and network security

This guide is not prescriptive. Rather, it can help managers prioritize risk and implement security measures.

C. Benefits of Security Effort

By investing time and money in security efforts, managers can reduce the likelihood of adverse effects on employees, the public, and the environment, as well as help their companies avoid costly losses. In effect, security is a tool for maintaining operations integrity. Even a small incident, such as threatening graffiti by an intruder, can leave employees too distracted to work well and can cost a significant sum to rectify. A large incident, such as a deliberate release of a site's hazardous materials, can injure people, harm the environment, and seriously damage a company by disrupting operations, inviting multimillion-dollar lawsuits, requiring costly remediation, upsetting employees, and injuring the company's reputation. If a risk assessment determines that an access control system and closed-circuit television surveillance are warranted, the cost of those systems is minimal compared to the costs that follow many serious security breaches.

Benefits of a Security Program

- Safeguards employees, the community, and the environment
- Maintains the integrity and effectiveness of operations
- Reduces litigation risk, insurance costs, and theft
- Reduces the risk of vandalism and sabotage by employees and non-employees
- Protects trade secrets
- Improves relationships with local authorities and surrounding communities
- Provides a mechanism for personnel control and accounting in case of emergency

Section 2: Risk Assessment and Prevention Strategies

The first step in constructing a solid security program is to conduct a risk assessment—in other words, to take stock of the assets that need to be protected, the threats that may be posed against those assets, and the likelihood and consequences of attacks against those assets. The chemical industry is unique in its approach to risk assessment because the security risks and needs of individual companies, and even those of individual facilities, can vary greatly from one to the next. Still, it is important to remember that attacks against chemical assets can hold greater consequences for the community than attacks on the assets of some other industries.

A. Assets

In security terms, assets are broadly defined as people, information, and property. At a chemical facility, the people include employees, visitors, contractors, haulers, nearby community members, and others. Information includes trade secrets (such as recipes, formulas, prices, and processes), other confidential business information, employee information, computer passwords, and other proprietary information. The range of property that a security effort might wish to protect includes the following:

- Buildings
- Vehicles
- Production equipment
- Storage tanks and process vessels
- Control systems
- Telephone and data lines
- Raw materials
- Finished product
- Electrical power lines
- Backup power systems
- Automated production equipment, such as digital control systems and programmable logic controllers
- Hazardous materials
- Boilers
- Water supply
- Sewer lines
- Waste treatment facilities and equipment
- Natural gas lines
- Rail lines
- Office equipment
- Supplies
- Tools
- Personal possessions

B. Threats, Vulnerabilities, and Consequences

Once assets have been evaluated, a security manager may want to consider which assets may be vulnerable. This procedure helps identify and prioritize likely targets and save companies from expending resources where the likelihood of attack is remote. For ex-

ample, companies involved in certain polymer markets may produce a suspension in which a powdered polymer is suspended in solution. Even if this product is made in significant quantities, it is an unlikely candidate for a terrorist target. Therefore, expending resources to counter a terrorist threat against that target would not be wise. How, then, do companies assess the likelihood that an asset would be a desirable target?

Since chemical companies routinely perform many different evaluations and assessments, this guidance attempts to build on those existing practices to provide a tiered approach to risk-based assessment. A tiered, risk-based approach is the most effective and efficient way to evaluate, identify, and prioritize potential targets. A tiered approach is nothing more than starting with simple evaluation techniques, usually qualitative in nature, and identifying areas in which more information would be useful to reach a risk-based conclusion.

A common type of assessment in the chemical industry is a chemical hazards evaluation, in which the hazards of a chemical are compared with the potential for exposure or potentially dangerous conditions. This comparison helps answer whether a given chemical is likely to cause harm. The comparison can begin with a simple, qualitative description of how and under what circumstances a chemical is manufactured and used. The assessor can then analyze the physical and chemical properties of the substance and quickly weed out less hazardous scenarios before prioritizing on the likelihood of the scenarios.

In addition to a chemical hazards evaluation, companies routinely perform a process hazard analysis (PHA). A PHA analyzes the potential causes and consequences of fires, explosions, releases, and major spills of chemicals. The PHA focuses on equipment, instrumentation, human actions, and external factors. These considerations help managers determine the hazards and potential failure points or failure modes in a process. This type of analysis could easily be adapted to a vulnerability assessment.

Another type of assessment used in the chemical industry is a security risk assessment. Security risk assessment focuses specifically on whether a company's security management program is adequate for protecting its assets. Physical and geographical factors, too, should be evaluated in the context of vulnerability.

One approach is described below that could be used by companies that want to perform a vulnerability assessment. Many practices performed by companies on a regular basis could easily be incorporated into this approach. This is not a prescriptive approach; instead, it is a suggested flow of thought and information. It is entirely conceivable that one or more steps would not apply to certain chemicals. It is up to the assessor to use professional judgment and determine the appropriate areas to be addressed.

Step 1: Chemical Hazards Evaluation

Chemical hazards evaluations are routinely performed in the chemical industry. They are often done in the context of the Responsible Care® Product Stewardship Code. Although they can and do differ in methodology, chemical hazards evaluations are designed to answer this two-part question: How likely is a chemical release, and how harmful would it be? These evaluations can easily be incorporated into a vulnerability assessment. Doing

so augments the assessment of a given facility and helps in evaluating whether it might be considered an attractive target.

Step 2: Process Hazard Analysis (PHA)

PHAs, are often done in the context of the Responsible Care® Process Safety Code and are considered good practice in the chemical industry. PHAs may be a good place to begin a vulnerability assessment for chemicals and processes of security concern. A PHA is designed to highlight areas of potential vulnerability, which, upon further study, may also be a potential target of an adversary.

Step 3: Consequence Assessment

Although it may be convenient to use worst-case scenarios and err on the side of safety, that approach is not practical for assessing all threats and appropriate countermeasures. Economics and common sense dictate that potential threats and consequences (as well as the actions to counter them) be prioritized.

Step 4: Physical Factors Assessment

After assessing the hazards and the likelihood that something could cause harm, it may be useful to address the physical factors that could affect the attractiveness of a potential target. These factors can potentially be used to reduce the likelihood that an object or location might be chosen as a target.

Some questions that can be asked include these:

- What size and type of container is it?
- Where is it located?
- Are the containers side-by-side, stacked, isolated?
- What surrounds the plant site, and at what distance?

Step 5: Mitigation Assessment

The information in risk management and emergency response plans can help managers assess factors that could mitigate the effects of a chemical release. The presence of effective risk management and emergency response plans may affect the likelihood that a facility is chosen as a potential terrorist target. For example, anhydrous ammonia is readily absorbed and controlled by a water fog. This reduces the likelihood that anhydrous ammonia will spread in its gaseous state to large areas, and thus could reduce its attractiveness as a target for terrorism.

Step 6: Security Assessment/Gap Analysis

After identifying potential vulnerabilities, threats, and countermeasures, the manager could then turn to a security assessment. This assessment helps identify whether the security policies and measures in place are appropriate for meeting the potential threat. Security audits are often performed to help determine whether protective measures are adequate. The person responsible for security at a company, if he or she is not primarily a

security professional, may want to consider consulting with security professionals for this part of the vulnerability assessment. Professional judgment is an integral part of the security assessment.

The following list identifies some of the potential threats that a chemical facility may wish to address:

- Loss of containment
- Sabotage
- Cyber attack
- Workplace violence
- Theft
- Fraud
- Product contamination
- Infiltration by adversaries
- Attack on a chemical plant as part of chemical and biological terrorism
- Assault
- Trespassers committing vandalism or setting fires for fun
- Thieves looking for precursor chemicals to use in illegal drug manufacture; break-in can also result in valves being left open, causing a chemical release
- Protesters disrupting plant operations through trespassing, vigils, assemblies, rallies, intimidation of employees, chaining selves to plant, or blocking traffic
- Bomb threats
- Workplace drug crime
- Theft of confidential information
- Hacking into information systems to disrupt computer-controlled equipment, causing an unplanned release of chemicals
- Product tampering
- "Hands-off" threats, such as cutting off electricity, telephone, or computer network, or else contaminating or cutting off water
- Vandalism of control rooms and equipment, and destruction of system documentation to make repair more difficult
- Disruption of cooling systems for electronic equipment rooms
- Creation of destructive or hazardous conditions through modification of fail-safe mechanisms or tampering with valves (done in person or electronically from a distance)

There is no one-size-fits-all approach to a vulnerability assessment, nor is there a one-size-fits-all approach to security. A multidisciplinary approach may benefit companies performing an overall vulnerability assessment. The professional judgment of security personnel, combined with environmental health and safety employees, process safety engineers, and process operators, can yield a comprehensive approach without draining scarce resources.

Preventing a Planned Attack

In December 1999, federal agents arrested two anti-government militia members in Elk Grove, California, in connection with a planned attack against a facility where 24 million gallons of liquid propane were stored. Federal officials said the threat to the plant had been eliminated even before the arrests, as extraordinary security precautions were put in place at the facility.

Experts differed on what effect a successful attack at the plant would have had. Some said a massive fire would have resulted but would have been contained within the plant's boundaries. Others said destruction and fires could spread a mile from the plant, reaching a high school, houses, and businesses.

The local sheriff ordered a special weapons and tactics team to stand guard at the plant day and night for at least a month after the threat was reported.

Company officials said the type of attack planned could not have detonated the propane tanks. Nevertheless, to protect the site, the propane company added numerous security devices in the weeks preceding the arrest, including a trench to protect the perimeter of the plant from a car-bomb attack. In addition, the company hired off-duty sheriff's deputies to help guard the facility and installed a new, double-gated entrance to stop unauthorized vehicle entry. The plant is circled by a chain-link fence topped with barbed wire. The plant also uses alarms and cameras that continually monitor sensitive areas of the facility.

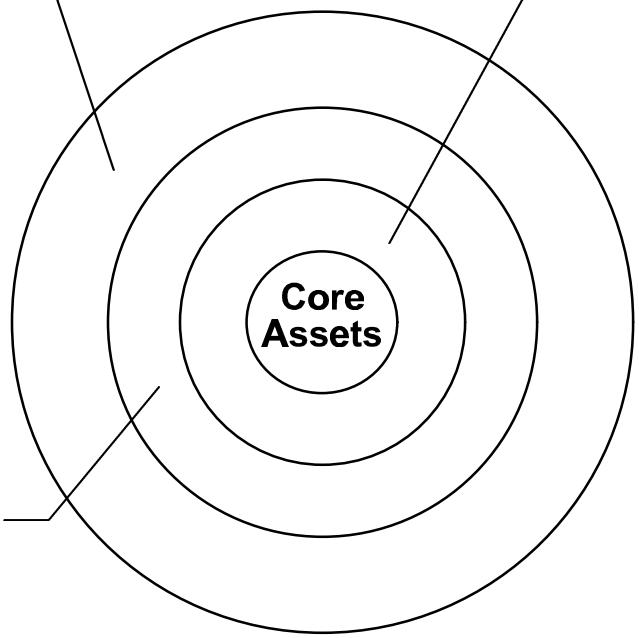
C. Prevention Strategies

Security tends to emphasize "rings of protection," meaning that, if possible, the most important or most vulnerable assets should be placed in the center of concentric levels of increasingly stringent security measures. For example, where feasible, a chemical facility's electronic control room should not be placed right next to the building's reception area; rather, it should be located deeper within the building so that, to reach the control room, an intruder would have to penetrate numerous rings of protection, such as a fence at the property line, a locked exterior door, an alert receptionist, an elevator with key-controlled floor buttons, and a locked door to the control room.

Another prevention strategy involves cooperation with law enforcement agencies, security staff in other companies, and fellow members of trade associations in order to share threat information. It is useful to know whether other chemical facilities in an area have experienced an intrusion so that appropriate security measures can be stepped up. Information sharing of that sort may also help in securing a conviction of the guilty parties.

The field of security employs many other prevention strategies, such as "crime prevention through environmental design" and security awareness programs for employees. This guide describes some of them, but interested managers may wish to learn more about security through further reading or by attending security training sessions.

Sample Rings of Protection



Outer Ring
- lighting
- fences
- gates
- bollards
- walls
- trenches
- intrusion detection sensors
- guards on patrol and posted at property-line access points

Middle Ring
- locked doors
- receptionist
- badge checks
- access control system
- window bars
- parcel inspection
- turnstiles

Inner Ring
- alert personnel
- door and cabinet locks
- network firewalls and password controls
- visitor escort policies
- document shredding
- access control devices
- emergency communications systems
- secure computer room
- motion-activated closed-circuit television

Section 3: Management Issues

At a particular chemical facility, security management responsibility generally should be assigned to one person. That person may or may not be called "security manager," but some person should be in charge of the security effort, even if he or she has other responsibilities. The person assuming the security role can perform a number of important security management functions, such as promulgating policy, establishing relationships with law enforcement agencies and surrounding communities to address security concerns, developing and managing incident reporting systems, boosting employees' security awareness, referring security breaches for investigation, coordinating emergency response, and periodically reassessing the site's security program.

A. Policy

A security effort works best when employees see it as an important part of the company's mission. Employees are more likely to see security as a company priority if the company's top management visibly supports security efforts. Among the best ways to demonstrate that support are to include security as one of the company's core values and to promulgate official company policies regarding security.

Security policies can be established on the site level or a company-wide level, and they can address a wide range of topics, such as the following:

- Access control
- Drug and alcohol use
- Workplace violence, threats, intimidation, and other misconduct
- Weapons-carrying by employees
- Pre-employment screening
- Information protection
- Locker searches
- Reporting of incidents and threats
- Response to bomb threats and suspicious packages
- Response to civil disturbances (including protest demonstrations)
- Ethics (requirement to report violations, etc.)

The Appendix contains sample policies addressing several of the preceding topics. They are intended only as examples, are not necessarily recommended in all their details, and may not be appropriate for all facilities.

B. Collaboration

Managers may wish to consider establishing partnerships or enhancing relationships with local, state, and federal law enforcement and other public safety agencies. Through such a network, managers may learn more easily of looming threats, dangerous trends, and successful and unsuccessful security measures. (See Appendix for information on Operation Cooperation, one approach to establish collaboration between the private sector and

public law enforcement.) It may also be possible to obtain threat and other information from Local Emergency Planning Committees, community advisory panels, mutual aid groups, and state chemical associations.

Benefits of a Working Relationship with Public Authorities

In one instance, demonstrators were upset at the cost of an AIDS drug and decided to conduct a protest at the corporate headquarters of the company that produced the drug. The protesters announced their plans to protest without a permit and to block traffic. They invited the media to attend, predicted a civil disturbance, and said they expected people to be arrested. In addition, they said they planned to dump contaminated blood at the doorstep of the corporation. Moreover, they requested that the police let them go after the media left and that the police escort the protesters in and out of the city.

However, because company staff had a working relationship with the city government and local police, they were able to convey the company's concerns to the authorities, and the company's interests were protected.

The actual course of events differed somewhat from the protesters' plans. The city did not want to allow the protest without a permit, but at the special request of the company, the city acquiesced. However, they were told their protest had to occur before or after the noon traffic hour. They were also told they would not be released if they were arrested for civil disobedience. At the company's request, police made arrests not in public view but inside the building, outside the view of the media. The result was a protest that inconvenienced but did not endanger the company.

Internal collaboration can also be important. By clarifying relationships and procedures with other management functions (such as employee safety and health, legal, and human resources), a manager may open information channels within the company and be able to provide a more coordinated response to security incidents.

Internal Collaboration

To be effective in a security leadership role, a manager must be proactive and be able to plan for and manage risk. Knowledge of whether and when the risks may change is critical. Other company departments can be a source of such information.

For example, a chemical company's public affairs department may be able to inform the security-responsible manager that a group is planning a protest at his or her facility and may even be able to obtain the protest's agenda and expected number of protesters. The human resources department may be able to contact managers about evolving security-related personnel issues, such as suspensions, terminations, labor unrest, or employees exhibiting unusual behavior. The purchasing or procurement department may be able to provide information about contractor or vendor changes that might have security implications (such as theft of equipment or tools). The legal and accounting departments may be able to inform managers about investigations of conflict of interest or misappropriation of funds.

At one chemical facility, the information technology department contacted managers responsible for security when the IT department began to plan a major computer equipment transition. Security concerns were taken into consideration early in the process. The new equipment was then properly secured during transport, upon arrival at the site, and while being installed, and the old equipment was accounted for and properly disposed.

It is generally considered important for interdepartmental relationships and information-sharing to go both ways. Security staff can also provide intelligence and advice to other company departments.

C. Incident Reporting and Analysis

By keeping detailed records of security incidents, managers may be able to spot trends and piece together facts that lead to successful investigations. Some security managers use incident management software, which has graphing, charting, and search functions that can help bring an offense or loss pattern to light and identify issues of security concern.

Incident data will only be available for analysis if incidents are reported and recorded. Managers may wish to establish several channels for incident reporting. For example, they may decide to promulgate the phone number and e-mail address of the person in charge of security. Some companies have set up anonymous employee hot lines to encourage employees to report suspicions. It may also be useful to make it obligatory for employees to report security incidents.

Anonymous Employee Hot Line

One large chemical company established a hot line to enable employees to report problems ranging from ethics violations to harassment. Sometimes the hot line is used by non-employees—usually terminated employees or friends of employees reporting something told to them by the employee, who was reluctant to report it to the company for fear of retaliation.

The hot line is publicized in various ways. It is touted in the employee code of conduct and in a letter from the company chairman posted permanently at all company facilities. The preferred method for employees to report wrongdoing is to bring it to the attention of their immediate supervisor. However, if the employee is uncomfortable with that approach, the hot line is available for anonymous reporting. All descriptions of the hot line stress that employees will not face retaliation for reporting wrongdoing.

The hot line has received calls alleging that a manager or supervisor was involved in a kickback operation with a vendor. In some cases, company investigations verified the schemes, making it possible for the company to take corrective action. Callers have also used the hot line to report concern that workplace violence may occur. Again, in several cases, investigations verified the callers' concerns, and corrective action was taken.

D. Employee and Contractor Training and Security Awareness

It is axiomatic in security that employees and contractors can serve as the eyes and ears of a company-wide security effort. Employees and contractors see much that occurs in and around a chemical facility and are in a good position to notice when something or someone does not seem quite right. Training and awareness measures can transform employees and contractors into a natural surveillance system.

Developing security awareness can also reinforce existing security practices, such as the following:

- Locking doors
- Looking for and reporting suspicious packages (see sample guidance in Appendix)
- Challenging people who are not wearing ID badges
- Not writing computer passwords on computers
- Not taping exterior doors open to facilitate outdoor smoking breaks

Managers may reinforce personnel training in security practices through e-mailed security reminders, security tips posted on a corporate intranet, advice and contact numbers in local and company-wide internal publications, and the distribution of security-related videos, pamphlets, tent-cards for lunch tables, posters, etc.

E. Investigations

Suspicious incidents and security breaches (of company policies) should be investigated by trained professionals. Site management should refer such incidents to corporate counsel or corporate security management. Any suspected illegal activity should be reported for referral to law enforcement, if appropriate.

The following are some types of security incidents that might warrant investigation:

- Doors not secured, holes in fence lines, indication of illegal entry
- Unauthorized egress by personnel in restricted areas of the facility
- Signs of vehicles in restricted areas along pipelines, fence lines, electrical substations, or remote plant security gates
- Individual asking for technical information about the facility that could be used by an adversary to cause harm
- Major unexplained process upsets
- Unexplained loss of containment of hazardous material
- Unexplained loss of raw material or product
- Major cyber attack against internal process control systems

F. Emergency Response and Crisis Management

Emergency response and crisis management are natural functions that security-responsible managers may perform for their companies. Proper crisis management may prevent an intrusion or attack from becoming a major incident. In the chemical industry, emergency response and crisis management functions are especially complicated, and the way in which they are performed is to a great extent dictated by government regulation. This section, therefore, does not attempt to specify how a company should respond to emergencies and manage crises.

Nevertheless, a few measures that managers may consider include the following:

- Develop an emergency response plan that fits the specific facility's needs and resources.
- Develop a system by which to account for employees and visitors during emergencies.
- To the appropriate degree, attempt to control the incident so that evidence will be preserved for later investigations.
- Develop a crisis communication system for key personnel and security staff so that they can (1) signal for help surreptitiously when necessary (with duress alarms, for example), (2) keep a small incident from escalating into a large one,

and (3) contact other key staff easily during a crisis (by means of intercoms, mobile and land-line telephones, e-mail, and two-way radios).

Sample emergency response plans for civil disturbances and bomb threats are presented in the Appendix.

G. Periodic Reassessment

The conditions surrounding a security effort change constantly. Employees come and go, a facility's contents and layout may change, various threats wax and wane, and plant operations may vary. Even such mundane changes as significant growth of bushes or trees around a facility's exterior may affect the security plan (for example, by providing cover for intruders).

Therefore, managers should review their security measures periodically, as well as whenever facilities or other conditions change significantly. It may also be useful to do the following at appropriate intervals:

- Update risk assessments and site surveys.
- Review the level of employees' and contractors' compliance with security procedures.
- Consider whether those procedures need modification.

It is also useful to establish ongoing testing and maintenance of security systems (such as access control, intrusion detection, and video surveillance).

Section 4: Physical Security

The term "physical security" refers to equipment, building and grounds design, and security practices designed to prevent physical attacks against a facility's people, property, or information. It is distinguished from cyber or network security, which is addressed in Section 6. Elements of a physical security effort may include access control, perimeter protection, intrusion detection, security officers, and other measures.

A. Access Control

The term "access control" generally refers to physical or behavioral measures for managing the passage of personnel and vehicles into, out of, and within a facility. An access control plan strives to exert enough control to protect the facility while still allowing employees enough freedom of movement to work effectively.

The appropriate level of access control varies significantly from facility to facility. It depends on the number of employees, hazards of materials present, level of pedestrian and vehicular traffic into and out of the facility, degree to which facility operations are controversial, attractiveness of the facility as a target of various threats, proximity of the facility to populated areas, and many other factors.

The following are just a few of the measures that managers may wish to consider for the purpose of controlling access into, within, and out of a chemical facility:

- Post "No Trespassing" and "Authorized Access Only" signs, along with signs stating that vehicles and visitors are subject to search.
- To the extent feasible, employ natural surveillance by arranging reception, production, and office space so unescorted visitors can be noticed easily.
- Install appropriate locks on exterior and interior doors.
- Keep publicly accessible restroom doors locked and set up a key control system. If there is a combination lock, only office personnel should open the lock for visitors. Keep closets locked.
- Require visitor sign-in logs and escorts.
- Pay close attention to access control at loading and unloading areas.
- Install appropriate, penetration-resistant doors and security hinges.
- Install secure windows with appropriate locks, perhaps using unbreakable plastics instead of glass and employing window bars.
- Institute a system of employee and contractor photo ID badges. Train employees to challenge persons who are not wearing badges.

- Establish a system for determining which cars, trucks, rail cars, marine vessels, and other vehicles may enter the site, through which gates, docks, or other entrances, and under what conditions. Such a system may be part of the pedestrian access control system, relying on key cards carried by vehicle operators, or it may be an independent system relying on staffed security posts.

- Install an electronic access control system that requires the use of key cards at main entrances and on other appropriate doors and that provides an audit trail of ingress and egress. Consider electronic access control for entry to motor control centers, rack rooms, server rooms, telecommunication rooms, and control rooms.

- Install a closed-circuit television system to monitor key areas of the facility. Where appropriate, employ motion sensors that mark the video recording and alert security staff when someone enters a restricted area.

- Institute a system of parcel inspection (using magnetometers, X-ray screening, or explosives detectors). Require the use of property passes for removal of property from the site.

B. Perimeter Protection

Controlling the movement of people within a facility is important, but it is far better to stop intruders—whether they be terrorists, saboteurs, vandals, thieves, protesters, or disgruntled former employees—at the edge of a facility's property, long before they reach vital assets and operational areas.

Perimeter protection includes such measures as these, which managers can consider and implement as appropriate:

- Fences and exterior walls that make it difficult for intruders to enter the site

- Bollards and trenches that prevent vehicles from driving into the site at points other than official entrances

- Vehicle gates with retractable barriers

- Personnel gates and turnstiles

- Setbacks and clear zones that eliminate hiding places near the site's perimeter, making it difficult for intruders to approach the site unnoticed

- Lighting that makes it easier for employees and even passersby to observe and possibly identify intruders

C. Security Officers

Security officers can provide a range of useful security services, such as touring a site to look for intruders or irregularities, staffing site entrances to check IDs, maintaining entry

and exit logs, handing out trucker safety lists, reminding employees and contractors of security and safety policies, and assisting in emergencies. Some security officers also have first aid and CPR training, boosting their companies' emergency response capabilities.

If it is deemed appropriate for a site to have security officers, managers should consider whether the officers will tour the site or remain at fixed posts; whether they will be contract or in-house officers; and what training and licensing they should receive. Managers should also develop "post orders," which are written directions informing security officers what they should do on the job.

Security personnel help chemical facilities with access control and emergency response, but they can also help in other ways. Because they patrol areas that may be unoccupied in the evenings and weekends, security officers can prevent problems that might otherwise go undetected until too late.

D. Backup Systems

From a security standpoint as well as a safety and operations standpoint, it may be appropriate for chemical facilities to secure such utilities as electricity, communications (telephone and computer), water, sewer, and gas. Crucial communications equipment and utility areas can be protected with locks and with alarms that ring to a location that is staffed around the clock. Wiring can be protected by being placed in rigid conduit so it cannot easily be cut.

Such key resources as control centers, rack rooms, computer servers, and telecommunications equipment may warrant a backup power source, such as a generator.

E. Other Considerations

At a chemical facility, managers should keep in mind that any physical security hardware must be safe for use in that particular facility. For example, closed-circuit television cameras and access control card readers may need to be specially selected so they are safe and effective in corrosive or flammable areas.

In addition, any site redesigns should be done with security in mind. For example, plants should generally be laid out so that the most vulnerable or important locations are hardest for adversaries to reach.

A few general physical steps that managers may wish to take include these:

- Keep offices neat and orderly to identify strange objects or unauthorized people more easily. Empty trash receptacles often.

- Open packages and large envelopes in executive offices only if the source or sender is positively identified.

- Keep closets, service openings, and telephone and electrical closets locked at all times.

Section 5: Employee and Contractor Security Issues

Sadly, it is possible for threats to chemical facilities to come from within as well as outside. Disgruntled employees and former employees sometimes pose a risk. Workplace violence can erupt from employees or contractors with violent tempers, from rejected intimate partners of employees, and even from disgruntled customers. Pre-employment background screening may help companies weed out job candidates who seem likely to cause trouble, and workplace violence policies, awareness, and response plans may help forestall other threats.

A. Hiring and Employment Termination Practices

Managers should consider using hiring and employment termination practices that contribute to the security of their facilities. For example, careful pre-employment screening might turn up a history of convictions for theft or violent crimes, of workplace violence or threatening behavior, or of interests inimical to the company. Some companies screen contract workers or require contracting companies to screen their own employees before they will be allowed on-site.

When a worker's employment ends, managers may want to keep in mind certain precautions:

- Treat the person with respect. It may be helpful to provide managers with sensitivity training and aggression management training.
- Retrieve the worker's keys, access control card, and company ID.
- Change combination locks and even some keyed locks.
- Change computer passwords.

For involuntary terminations of employment, the following additional steps should be considered:

- When possible, assess the worker's violence potential before termination and, if appropriate, take additional security precautions.
- Direct the worker to the company's employee assistance program and outplacement services.
- Escort the departing worker out of the building to make sure he or she does not harm data, property, or people on the way out.

See the sample pre-employment screening policy in the Appendix.

B. Workplace Violence Prevention and Response

Workplace violence prevention fits well with a company's other efforts to ensure employee safety. It also uses methods related to traditional physical security. For example, security staff attempt to stop attacks from the outside by employing "rings of protection," halting intruders several stages before they reach key assets and work areas. In the same way, some companies attempt to stop workplace violence several steps before anyone is injured. They do so by taking action not only against violence but also against threats and intimidation, which might lead to violence.

The following list identifies some measures that managers may wish to consider in preventing and responding to workplace violence:

- Adopt a policy of prohibiting (and responding to all reports of) physical violence, verbal abuse, willful destruction of company property, and intimidation. Consider suspending suspects from work while the reports are investigated. Respond to confirmed reports with counseling, reprimands, or termination of employment.

- Teach employees how to recognize the early warning signs of a troubled or potentially violent person and how to respond.

- Require employees who have obtained court-issued restraining orders to notify management immediately. Managers can then take steps to protect all employees and can notify law enforcement of any violations.

- Limit former employees' access to the workplace as appropriate.

- Establish policies forbidding the use and possession of drugs at any time and the possession of alcohol and weapons at work.

- Train managers on appropriate ways to handle difficult employee terminations, layoffs, and discipline.

- After a violent incident, evaluate the potential for further violence at the facility.

- Help employees with the psychological consequences of workplace violence. Doing so not only is humane but also helps reduce losses caused by absence, loss of productivity, and workers' compensation claims.

- Support prosecution of offenders by accommodating employees who are needed for court appearances and cooperation with the prosecution.

- To avoid a defamation suit by accused employees who turn out to be innocent, managers should investigate allegations quickly and quietly.

See the Appendix for a sample policy on workplace violence.

Section 6: Information, Computer, and Network Security

In a chemical facility, protecting information and computer networks means more than safeguarding a company's proprietary information and keeping the business running, as important as those goals are. It also means protecting chemical processes from hazardous disruptions and preventing unwanted chemical releases. To an adversary, information and network access can equal the power to harm the company, its employees, and the community at large.

A. Operations Security

The chemical industry well understands the importance of protecting its trade secrets. However, it is also vital to protect information that could be useful to criminals, demonstrators, and terrorists who wish to plan attacks on a chemical site or obtain hazardous materials for weapon-building. Examples of such information include these:

- Process flow diagrams
- Piping and instrument design diagrams
- Formulations
- Recipes
- Client and supplier lists
- Site maps
- Other information that describes the workings of a chemical facility

One approach to denying adversaries the information they seek is called Operations Security, or OPSEC. In using OPSEC, managers take these steps:

1. *Identify critical information.* What would an adversary need to know about the site's operations in order to penetrate the site, damage the site, harm personnel, or release or steal hazardous materials?

2. *Conduct a threat assessment.* What persons or groups have the desire and capability to attack the site or release or obtain product?

3. *Perform a vulnerability analysis.* What are the weak points in the site's overall armor? How could an adversary enter the facility? How could an adversary obtain the information he needs to carry out his plan? Could an adversary develop the information he needs by combining small, seemingly insignificant data that is publicly available? Do the company's websites, government-required filings, and annual reports divulge more than is necessary?

4. *Assess the risk.* Weighing the threat (level of adversary's desire and abilities) and vulnerability (weak points in the site's defenses), what is the probability that the adversary will succeed in his attack? What would be the effect of the adversary's success?

5. *Apply countermeasures.* See the following sections on security of spoken information, documents, and computers and networks.

B. Spoken-Information Security

Depending on the threat level, managers may wish to consider the following measures:

- Prohibit radio conversations about sensitive topics.
- Alternatively, use voice encryption for radio conversations. (However, such encryption should be used either always or never. If it is used only sometimes, the adversary may be able to determine *when* sensitive information is being discussed, even if he cannot determine the content of the conversation. OPSEC considers even that information potentially useful to an adversary.)
- Conduct the most sensitive conversations in person.
- Prohibit employees from giving out potentially risky information over the phone, as one may not be sure to whom one is speaking.

C. Document Security

Depending on the threat level, managers can consider taking some of the following steps:

- Shred documents.
- Lock file cabinets and trash bins.
- Institute a clean desk policy.
- Mark sensitive documents as "confidential."
- Provide employee training and reminders about document security practices.

D. Computer and Network Security

Managers can choose from a wide range of measures for enhancing computer and network security at their facilities. Options include the following:

- Physically secure computer rooms, motor control centers, rack rooms, server rooms, telecommunications rooms, and control rooms, ideally with electronic or biometric access control systems that record ingress and egress.
- Employ firewalls, virus protection, encryption, user identification, and message and user authentication to protect both the main computer network and any subsidiary networks, such as access control systems, that are connected to it or to the outside.
- Teach employees to beware of ruses to obtain their computer passwords.
- Require systems administrator to disable all Internet connection software that may be prepackaged in operating systems.

- Allow the principles of "least access," "need to know," and "separation of functions" guide the determination of user authorizations, rather than position or precedent.

- If possible, place the computer room above the first floor of the building to reduce the likelihood of theft and water damage (from broken water lines, floods, or fire fighting). The computer room should not be adjacent to an exterior building wall.

- Do not post signs indicating the location of the computing facility.

- Equip the computer room with adequate communications capabilities to facilitate prompt reporting of emergencies.

- Allow only authorized personnel to have physical access to central computer rooms. Supervise any visitors.

- Do not give keys or lock combinations to visitors.

- Require employees to notify management in advance if they wish to gain entry to the computing facility during hours when they are not scheduled to be working.

E. Audits and Investigations

To detect computer intrusions, managers can make sure that computer systems maintain an audit trail of access to system resources. Then they can regularly analyze transaction histories, looking for variances from the norm. In addition to checking users' authorizations, managers can pay attention to unusual times, frequency, and length of access.

Investigating computer intrusions is a complicated specialty. Before an incident occurs, the facility or IT manager may wish to line up a source of computer forensic assistance.

Section 7: Getting Started

This guide names some of the steps that managers may want to consider taking to protect their facilities. It does not attempt to be exhaustive, but only to outline some of the general approaches to chemical facility security. This section provides two condensed sample approaches to site security. The first sample is a site security analysis worksheet. The second is the Responsible Care® Security Model.

A. Sample Site Security Analysis

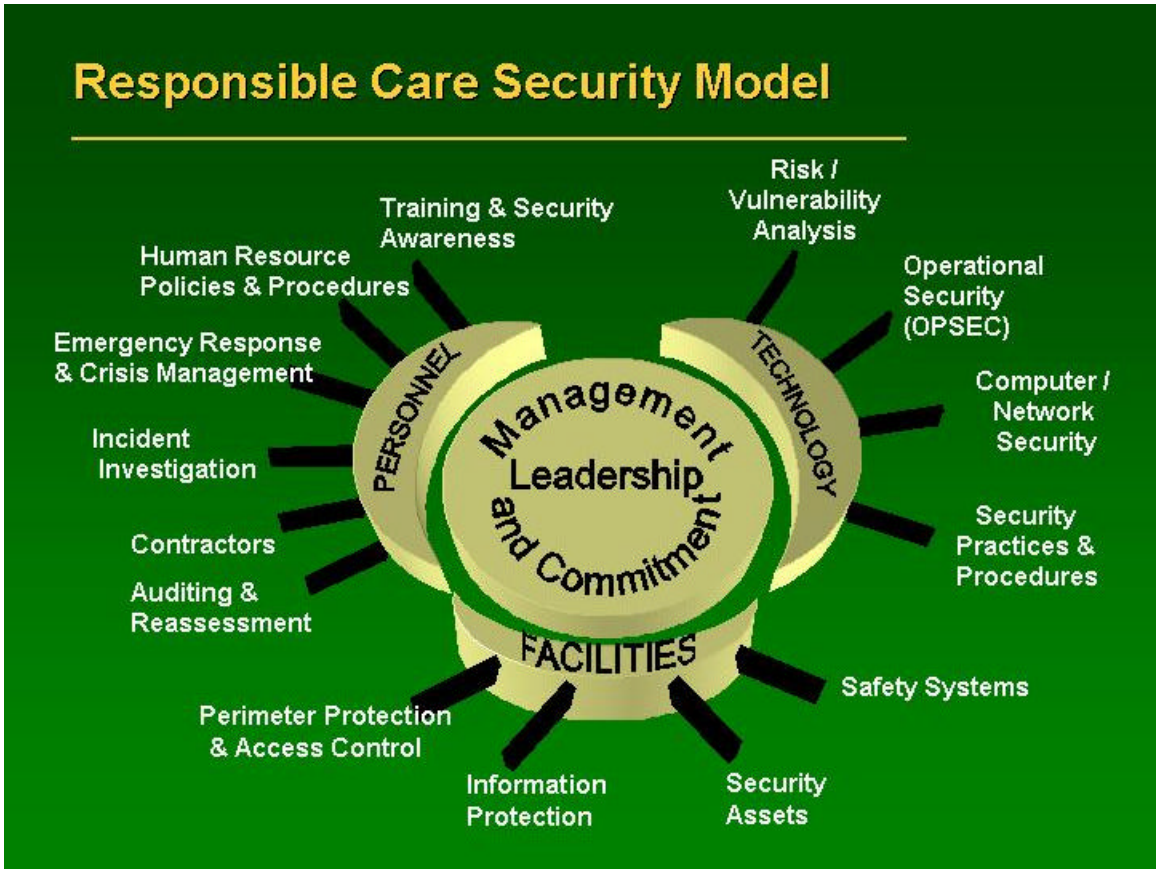
This sample follows the topical order in the preceding sections of this guide. This worksheet is a guide and not intended to be all inclusive.

Item #	Question	Response	Recommendations
A. Risk Assessment and Prevention Strategies			
1	Have we identified all key facility assets?		
2	Have we performed a chemical hazards evaluation?		
3	Have we performed a process hazard analysis?		
4	Have we performed a consequence assessment?		
5	Have we performed a physical factors assessment?		
6	Have we performed a mitigation assessment?		
7	Have we performed a security assessment/gap analysis?		
8	Have we developed rings of protection?		
B. Management Issues			
1	Does the company's top management visibly support security efforts?		
2	Have clear security policies been developed and promulgated?		
3	Have we established partnerships with local, state, and federal law enforcement agencies, other public safety agencies, and surrounding communities?		
4	Have we clarified relationships and procedures with other management functions to provide a more coordinated response to security incidents?		
5	Do we have a well-understood system for employees to report security incidents?		
6	Do we have a system for collecting and analyzing reports of security incidents?		
7	Have we developed security awareness programs for employees and contractors?		
8	Have we developed a procedure for referring suspicious incidents and breaches of company policy to corporate counsel or corporate security management?		
9	Have we developed a policy of referring all suspected illegal activity to law enforcement?		

Item #	Question	Response	Recommendations
10	Have we developed procedures for emergency response and crisis management?		
11	Do we periodically reassess the site's security posture (threats, vulnerabilities, risks, and countermeasures)?		
C. Physical Security			
1	Have we implemented appropriate access control measures, such as signs, secure doors and windows, locks, card-based access control systems, parcel inspection, and control of gates and docks?		
2	Do we have appropriate perimeter protection, using, for example, fences, bollards, trenches, turnstiles, and security lighting?		
3	Do we need security officers, on patrol or at fixed locations? If so, do they have written post orders to direct their activity?		
4	Have we appropriately protected crucial communications equipment and utilities?		
D. Employee and Contractor Security			
1	Have we developed appropriate security practices for voluntary and involuntary terminations of employment?		
2	Have we adopted policies and established procedures to prevent and respond to workplace violence?		
E. Information, Computer, and Network Security			
1	Have we taken steps (through the Operations Security, or OPSEC, process) to protect information that could be of use to our adversaries?		
2	Do we follow procedures to reduce the likelihood that spoken information (in face-to-face conversations, phone calls, and radio communications) could be picked up by adversaries?		
3	Do we follow appropriate procedures for protecting and destroying sensitive documents?		
4	Are we using appropriate hardware, software, and procedural techniques for protecting our computers and networks?		
5	Do we periodically analyze computer transaction histories to look for irregularities that might indicate security breaches?		

B. Responsible Care® Security Model

The Responsible Care® Security Model presented below summarizes one approach to chemical site security. Points of synergy between the Responsible Care® Security Model and the earlier sections of this document are noted.



The Foundation (see Site Security Guidelines [SSG] Section 3)

- Leadership by senior management through policy, participation, communications, and resource commitments
- Clear accountability for security across the organization
- Security readiness measured, audits conducted, and improvements implemented
- Dialogue with appropriate local, state, and federal law enforcement agencies to understand potential threats, conduct vulnerability assessments, and apply reasonable countermeasures
- Reporting, investigation, and appropriate corrective actions and follow-up on each security incident

- Sharing of relevant lessons learned from incidents and investigations within industry, government, and the community

Risk/Vulnerability Analysis (see SSG Section 2)

- Dialogue and partnership with local, state, and federal agencies to understand potential security threats
- Analysis of risks and vulnerabilities associated with potential threats
- Updating of risk/vulnerability analysis periodically and when threat information is revised
- Application of prevention strategies and countermeasures to mitigate a potential threat

Operations Security (OPSEC) (see SSG Section 6)

- Identification of critical information readily available to employees, contractors, and the public
- Threat/vulnerability analysis and risk assessment
- Application of prevention strategies and countermeasures to mitigate a potential threat
- Periodic revalidation of OPSEC analysis

Computer/Network Security (see SSG Section 6)

- Physical security for computer rooms, network routers, motor control rooms, telecommunications resources, and control rooms
- Firewalls, virus protection, encryption, user identification, and passwords

Security Practices and Procedures (see SSG Section 3)

- Current, complete security procedures for site employees, contractors, and security personnel

Training and Security Awareness (see SSG Section 3)

- Security awareness program
- Security training for all employees on recognition of potential threats and site security procedures

Human Resource Policies and Procedures (see SSG Section 5)

- Appropriate pre-employment screening for employees and contractors
- Programs designed to assure that employees in safety-critical jobs are fit for duty and are not compromised by external influences
- Workplace violence prevention and response programs
- Employment termination policies and practices

Emergency Response and Crisis Management (see SSG Section 3)

- Current, written emergency response plan including security elements, consistent with the Community Awareness and Emergency Response (CAER) Code
- Coordination of the written facility emergency response plan with the comprehensive community emergency response plan for reacting to a terrorist incident
- Periodic emergency response exercises testing the operability of the written plan to a security threat
- Company crisis management plan to support the response of the facility and community in the event of a significant security incident

Incident Reporting and Investigation (see SSG Section 3)

- Formal, systematic approach to evaluating and continually improving the security of the facility, understanding the causes of security incidents, and taking action to eliminate their recurrence

Contractors (see SSG Section 4)

- Contractor compliance with all facility security policies and procedures
- Contractor permission to enter given only with the authority of approved site personnel
- Display, at all times, of evidence of permission to enter the site

Auditing and Reassessments (see SSG Section 2)

- Arrangements to regularly check boundaries and other sensitive areas for unauthorized entry of personnel and materials
- Periodic audits of company security measures to assess security procedures and determine whether modifications are needed
- Periodic review of the effectiveness of procedures and systems to identify health and safety concerns through analysis of reports and records and undertaking of physical security system surveys

Perimeter Protection and Access Control (see SSG Section 4)

- Protection of vulnerable area perimeters based on the facility threat/vulnerability assessment
- Identification of all personnel, including visitors and contractors, by a badge or other means
- Controlled entry and exit of personnel and vehicles
- Records of entry and exit

Information Protection (see SSG Section 6)

- Identification, control, and securing of sensitive information

Security Assets (see SSG Section 2)

- Training of those with day-to-day security responsibility
- Operation by procedure and protocols
- Continuous evaluation for improvement opportunities
- Development and maintenance of communications and partnerships with local law enforcement agencies and inclusion of law enforcement representatives in facility drills

Process Systems (see SSG Section 2)

- Inclusion of process systems and equipment in the threat/vulnerability analysis
- Ability to safely shut down process systems and equipment during security incidents and emergencies
- Sufficient layers of protection through technology, facilities, and employees to prevent a catastrophic event

Section 8: Helpful Resources

A. Associations

American Chemistry Council
1300 Wilson Blvd.
Arlington, VA 22209
Phone: (703) 741-5000
Fax: (703) 741-6000
www.americanchemistry.com

The Chlorine Institute, Inc.
2001 L Street, N.W., Suite 506
Washington, DC 20036
Phone: (202) 775-2790
Fax: (202) 223-7225
www.cl2.com

Synthetic Organic Chemical Manufacturers Association
1850 M St. N.W., Suite 700
Washington, DC 20036
Phone: (202) 721-4100
Fax: (202) 296-8120
www.socma.com

American Society for Industrial Security
1625 Prince Street
Alexandria, VA 22314
Phone: (703) 519-6200
Fax: (703) 519-6299
www.asisonline.org

Internet Security Alliance
2500 Wilson Boulevard
Arlington, VA 22201
Phone: (703) 907-7090
Fax: (703) 907-7971
www.isalliance.org

State Chemical Associations

Alabama Chemical Association
Phone: (334) 260-7772
Fax: (334) 260-7775
www.AlaChem.org

Chemical Industry Council of California
Phone: (916) 609-9394
Fax: (916) 564-9398
www.cicc.org

Chemical Industry Council of Delaware
Phone: (302) 655-2673
Fax: (302) 655-4374

Florida Manufacturing and Chemical Council
Phone: (850) 224-4141
Fax: (850) 224-5238
www.fmcc.org

Chemical Industry Council of Illinois
Phone: (217) 522-5805
Fax: (217) 522-5815
www.cicillinois.org

Chemical Industry Council of Associated Industries of Kentucky
Phone: (502) 491-4737
Fax: (502) 491-5322

Louisiana Chemical Association
Phone: (225) 344-2609
Fax: (225) 343-1007
www.lca.org

Chemical Industry Council of Maryland
Phone: (410) 974-4797
Fax: (410) 974-4071
www.cicmd.org

Massachusetts Chemical Technology Alliance
Phone: (617) 451-6282
Fax: (617) 695-9568
www.masscta.org

Michigan Chemical Council
Phone: (517) 372-8898
Fax: (517) 372-9020
www.mccinfo.org

Minnesota Chemical Technology Alliance
Phone: (612) 332-8063
Fax: (612) 332-2089
www.minncta.org

Chemical Council of Missouri
Phone: (573) 636-2822
Fax: (573) 636-9749
ww.ccmo.org

Chemical Industry Council of New Jersey
Phone: (609) 392-4214
Fax: (609) 392-4816
www.cicnj.org

Alliance of Chemical Industries of New York State, Inc.
Phone: (518) 427-7861
Fax: (518) 427-7008
www.nyschemicalalliance.org

Manufacturers and Chemical Industry Council of North Carolina
Phone: (919) 834-9459
Fax: (919) 834-8268
www.mcicnc.org

Ohio Chemistry Technology Council
Phone: (614) 224-1730
Fax: (614) 224-5168
www.ohioche.org

Pennsylvania Chemical Industry Council
Phone: (717) 232-6681
Fax: (717) 232-4684
www.pcic.org

South Carolina Chemical Industry Council, South Carolina Manufacturers Alliance
Phone: (803) 799-9695

Chemical Industry Committee, Tennessee Association of Business
Phone: (615) 256-5141
Fax: (615) 256-6726
www.tennbiz.org

Texas Chemical Council
Phone: (512) 646-6401
Fax: (512) 477-5387
www.txchemcouncil.org

Chemical Industry Committee, West Virginia Manufacturers Association
Phone: (304) 342-2123
Fax: (304) 342-4552
www.wvma.com

Wisconsin Chemical Industry Council, Wisconsin Manufacturers and Commerce
Phone: (608) 258-3400
Fax: (608) 258-3413

B. Federal Agencies

National Infrastructure Protection Center
J. Edgar Hoover Building
935 Pennsylvania Ave., N.W.
Washington, DC 20535
Phone: (202) 323-3205
www.nipc.gov

U.S. Environmental Protection Agency
Office of Chemical Emergency Preparedness and Emergency Response
1200 Pennsylvania Ave., N.W.
Washington, DC 20460
Phone: (202) 260-2090
www.epa.gov/ceppo

U.S. Department of Labor
Occupational Safety and Health Administration
200 Constitution Ave., N.W.
Washington, DC 20210
Phone: (202) 693-2092
www.osha.gov

U.S. Department of State
Office of the Coordinator for Counterterrorism
Office of Public Affairs
Room 2507
2201 C Street, N.W.
Washington, DC 20520
www.state.gov/www/global/terrorism

U.S. Department of Justice
Office of Justice Programs
Terrorism and Domestic Preparedness
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
www.ojp.usdoj.gov

C. Publications

Counterterrorism and Contingency Planning Guide. Special publication from *Security Management* magazine and American Society for Industrial Security, 2001.

Dalton, Dennis. *Security Management: Business Strategies for Success.* Newton, MA: Butterworth-Heinemann Publishing, 1995.

Fennelly, Lawrence. *Handbook of Loss Prevention and Crime Prevention (3d)*. Newton, MA: Butterworth-Heinemann Publishing, 1996.

Fischer, R., and G. Green. *Introduction to Security (5th).* Stoneham, MA: Butterworth-Heinemann Publishing, 1992.

Jones, Radford W. *Critical Incident Protocol: A Public and Private Partnership*. Michigan State University: 2000.

Moritz, Milton E., ed. *CPP Study Guide, Revised 10th Edition*. Alexandria, VA: American Society for Industrial Security. As preparation for Certified Protection Professional exam, this book covers emergency planning, investigations, legal aspects, personal and physical security, protection of sensitive information, management, substance abuse, loss prevention, and liaison with law enforcement.

Operation Cooperation: Guidelines for Partnerships Between Law Enforcement and Private Security Organizations. Operation Cooperation is a national initiative to encourage partnerships between law enforcement and private security professionals. Its details are explained in a booklet and video, produced in 2000, available from the Bureau of Justice Assistance of the U.S. Department of Justice (www.ojp.usdoj.gov/bja). The booklet is available on-line at www.asisonline.org/opcoop.pdf.

Walsh, Timothy J., and Richard J. Healy, eds., *Protection of Assets Manual* (Santa Monica, CA: Merritt Co.). Four-volume loose-leaf reference manual, updated monthly.

D. Sample Plans, Policies, and Procedures

The following pages present several sample plans, policies, and procedures regarding specific security issues. The samples may serve as templates for a company's own, customized version. These are the policies presented:

- Sample Emergency Response Plan for Civil Disturbances
- Sample Guidance on Suspicious Letters and Packages
- Sample Bomb Threat Procedures
- Sample Pre-employment Screening Policy
- Sample Workplace Violence Policy
- Sample Employee Misconduct Policy
- Sample General Weapons Policy
- Sample Policy on Drug and Alcohol Use
- Sample Compact, Unified Security Policy and Procedures (two versions)

The sample policies are intended only as examples, are not necessarily recommended in all their details, and may not be appropriate for all facilities.

1. Sample Emergency Response Plan for Civil Disturbances

Civil disturbances and trespass on company property may be designed to impede normal operations or interfere with employee access to the facility. They are also often intended to maximize media interest. Protest activities may include, but are not limited to, any or all of the following:

- Pre-arranged, lawful assemblies, vigils, or rallies
- Unlawful, but nonviolent, acts of civil disobedience (e.g., symbolic trespassers and traffic blockages)
- Covert entry into facilities to conduct protest acts (e.g., post banners and paint slogans)
- Attempts to penetrate facilities or board vessels
- Rioting and destruction of property

A facility's emergency plan should be in place to deal with protests. Proactive steps should be taken to assess security risk for demonstrator activities and to define critical areas. Focus should be on preventing access to facilities. In the event entry into a company facility does occur, safety of personnel and operations is the highest priority. Because of this, demonstrators should be removed from the facility safely and quickly by local law enforcement officials, in accordance with local regulations and practices. In no event should demonstrators be allowed to remain in critical areas. The following guidelines have been identified as sound security practices and should be incorporated in response planning.

Access Control/Physical Security

- Establish alternate access control points for employee/contractor entrance to and egress from the facility; develop procedures for how access control will be handled at alternate points.
- Identify alternate routes for product transfer during demonstrations.
- Review existing safeguards and security practices to ensure adequate perimeter fencing, lighting, and protective force allocation or augmentation to respond to demonstrators blocking access or penetrating the facility.
- Ensure there is adequate physical security for critical facility doors and windows.
- Provide panic alarms linked to facility security control center for operators in critical facilities.

Protect Critical Areas / Define and Use Containment Areas

- Identify critical safety and operational sensitive areas and "non-critical" containment areas for peaceful demonstrators while injunction and legal recourse is being sought. It is recognized that in some jurisdictions our major facilities are considered strategic assets and the authorities will take appropriate action on that basis.
- Identify what is needed to seal off critical areas; develop a plan to use facility personnel to enhance protection at critical areas.
- Police and other local authorities should be used to remove non-peaceful demonstrators from the facility and to assist in channeling or moving peaceful demonstrators to non-critical areas.

Response Planning and Execution

- Maintain or improve liaison with local law enforcement.
- Work with local law enforcement officials to ensure that safety and security risks involving unauthorized personnel in [Company Name] facilities are promptly and appropriately dealt with.
- Plan in advance with local law enforcement agencies what specific actions can be taken to remove demonstrators quickly and safely from the facilities.
- Review the penal code to identify illegal actions that constitute non-peaceful behavior.

- Have a specific security plan to address lawful demonstrations as well as demonstrator trespassing, including crowd control and a response plan that maintains a non-confrontational approach while evaluating the safety exposure of demonstrators, site personnel, and the community.
- Ensure that radio and telephone contact with local law enforcement is functional.
- Review and update protective force procedures and response to demonstrators.
- Develop plans to augment the guard force in order to increase roving patrols during demonstrations, staff alternate access points, and protect critical areas.
- Train protective force and selected facility personnel to respond to unauthorized access using non-confrontational crowd control techniques.
- Train the protective force to refer all questions from the media or demonstrators to the [Company Name] public affairs representative or facility spokesperson.
- Update emergency response manuals with a protocol for managing demonstrations.
- Review planned countermeasures with the legal department. Legal action against demonstrators should be pursued, including allegations of illegal trespass and recovery of damages for site disruptions.
- Teach all site personnel what to do and what not to do during demonstrations.
- Review facility shutdown plans for adequacy and accuracy.
- Update contingency plans to include recovery plans for loss of critical assets.
- Conduct regular simulation drills and emergency response exercises; include local authorities.
- Train operations and management personnel to respond to civil disturbance scenarios. This may require some managers or supervisors to assume non-traditional roles, such as augmenting the protective force to secure critical areas until protective force augmentation or police or other local authorities arrive on the scene.
- Conduct an operational readiness and safety review before restarting activities in occupied areas.

Public Affairs Planning and Response

- Review public affairs guidelines.
- Identify a location away from critical areas where demonstrators can present a petition or statement to local management if deemed appropriate.
- Identify and prepare a site public relations representative to handle demonstrators' concerns.
- Identify and prepare a site public relations representative to handle questions from the media.
- Ensure proper notification of local management and appropriate [Company Name] business contacts.
- Determine the local legality of taking demonstrators' names and photos. Take names, photos, and video if allowed.

Threat Assessment

- Conduct a regional threat evaluation to assess the evolution of demonstrator activities on an ongoing basis.
- Institute information gathering and threat analysis to track local and regional concerns.
- Monitor intelligence sources through law enforcement contacts, consultants, the Internet, and activist publications and communications, and keep the [Company Name] Security Department informed of all significant changes. Increase security when warranted.

Critical Areas

Generally, critical areas include:

- Control rooms or centers
- Substations and electrical equipment
- Instrument air systems
- Process unit on sites
- Unit tankage
- Boiler houses and utilities
- Environmental treating operations (separators, processing equipment, discharge points)
- Flares and stacks
- Docks (during unloading and loading)
- Inside offices or shops in occupied buildings
- Off-site tankage (with toxic gas present)

Areas where demonstrators might be channeled (in order of preference) include:

- Open or surplus land
- Parking lots
- Interior roads
- Exterior of office buildings or shops
- Landfarms
- Wastewater lagoons or open water storage
- Docks when not in use
- Loading racks (for tank cars or tank trucks)
- Remote pipe racks
- Remote cooling towers

2. Sample Guidance on Suspicious Letters and Packages

The considerations below apply to letters and packages that might contain bombs or hazardous chemical or biological materials.

Workplaces tend to receive a great number of letters and packages every day. However, not even one piece in a million contains a bomb or chemical or biological material designed to harm the recipient, and closely analyzing each piece would drastically slow down delivery. Furthermore, there is no way to prevent dangerous letters and packages from being sent. Detection and interception are the only responses possible.

A prudent, risk-based approach to detecting dangerous letters and packages is likely to involve general, initial screening by the mail clerk. Possible indicators of suspicious mail include the following:

- Lumps, bulges, protrusions, or lopsidedness
- Unusual rigidity or bulk (in an envelope)
- Handwritten or poorly typed addresses or labels
- Use of string to bind a package
- Excess postage (suggests the object was not weighed by the Post Office or a company mailroom)
- Lack of postage or uncanceled postage
- Mismatching postmark and return address
- Any foreign writing, address, or postage
- Handwritten notes, such as: “To Be Opened in the Privacy of...,” “PERSONAL,” “CONFIDENTIAL,” or “Prize Enclosed”
- Incorrect spelling of common names, places, or titles
- Generic or incorrect titles
- Leaks, stains, strange odor, or protruding wires, string, or tape
- No return address or nonsensical return address
- Arrival before or after a phone call from an unknown person asking if the item was received

Mail that does not pass the simple, initial test should be subjected to interception (removal from the mail flow) and follow-up screening. To conduct follow-up screening, the screener could ask the recipient whether he or she was expecting the package, call the apparent sender, or use screening technology. If the screener is still concerned after taking those steps, he or she should report those concerns as directed by the company. The screener also should not open, shake, sniff, or taste the package or its contents.

3. Sample Bomb Threat Procedures

The most popular method of making bomb threats is by telephone. It is important that as much information as possible be received from the caller. All bomb threats should be taken seriously. However, experience has shown that most anonymous threat calls are a hoax, intended to create an atmosphere of anxiety and panic in order to interrupt normal activities. Therefore, absent positive target identification (PTI) indicators or other credible information, an evacuation may not be considered appropriate.

Threats by Phone

All persons who could receive a telephone bomb threat should be taught how to handle the situation effectively. In the event a call is received, the following procedure should be followed:

- Stay calm, be courteous, and do not display fear.
- Activate telephone recording unit, if available.
- Listen carefully. During or immediately after the conversation, take notes of the exact time the call was received, the exact words of the caller, and all details such as sex of caller, accent, attitude, background noises, and motive. Use a bomb threat checklist to record the details of the call.
- Advise the caller that the building, plant, or facility may be occupied and the explosion could result in death or serious injury to many innocent people.
- Keep the caller talking; the more he or she says, the more helpful the information. If the caller does not indicate the location of the bomb or the time of detonation, ask him or her what time it is to go off and where it is located.
- After the phone call, notify the appropriate facility staff.
- Do not discuss the call with anyone else unless authorized to do so or required by law.

Threats by Mail

Following are the instructions on how to handle bomb threats received by mail. The most likely recipients are mail room personnel and secretaries.

- Place all papers and envelopes associated with the threat in a bag or large envelope (clear plastic bag if possible). Pick up any bomb threat note ONLY by the edge.
- Do not handle the written threat any more than absolutely necessary.
- Do not allow anyone else to touch the note unless specifically authorized by a security representative or senior management.

Manager's Responsibility

In all cases of bomb threat, the facilities or security manager should assess the seriousness of the threat using the following bomb threat assessment and bomb threat response guidelines. He or she should also, if appropriate, notify law enforcement authorities.

Bomb Threat Assessment

Is the threat credible?

Consider:

- Time of day and day of week
- Mode—telephone or mail
- Identity of caller—child, female/male, young/old, drunk, foul language
- Specificity of the threat—time, location, type of explosive device
- Possibility of access to allow placing of the device

Does the threat contain Positive Target Identifications (PTIs)?

Did caller identify:

- Time the bomb is to detonate?
- Target to be destroyed?
- Bomb's construction, shape, or description?
- Bomb's location?

Bomb Threat Response

What is the proper response?

Do not evacuate?	This may be an appropriate response if there have been a number of recent, publicized hoax bomb threats in the area; if the caller seemed to be drunk; if the caller was a young child, or if it is a beautiful Friday afternoon about an hour or so before quitting time. This is especially true when no PTIs were provided in the bomb threat call.
Conduct a limited or general search of the facility?	Searches are usually the most appropriate choice and should generally be the chosen response, especially if no PTIs or only one PTI was given in the threat.
Order limited evacuation, general evacuation, or move to a safe haven?	Evacuations are usually ordered only when the call is judged to be serious, the threat credible, there is insufficient time to conduct a thorough search, and the judgment is made that employees will be at less risk evacuating or moving to a safe haven than remaining in place and seeking cover. **If two or more PTIs are given in the bomb threat call, an evacuation may be in order.**

How should the chosen response be executed?

- Use a PA announcement, telephone cascade, messenger, or other local notification plan.
- Determine who is to search and in what area. In general, employees should search their own area to determine if there are any suspicious objects. Common areas should be searched by those most familiar with the areas.
- Notify public law enforcement and emergency services as appropriate; notify immediately if a suspicious object is found.
- If appropriate, determine who is to be evacuated and to what location.
- If evacuation is ordered before a search is done, determine for how long. Consider options if weather is inclement. Consider possible effect on operations if evacuation occurs at or near shift change.
- Ensure that procedures are in place to account for all persons ordered to evacuate and determine that they have in fact evacuated and there is an orderly shutdown of operations, if required.
- Coordinate with local authorities to determine if the area needs to be searched and who will determine that operations can resume and people can return to their work stations.

Search Plans

A predetermined search should be organized. It is not effective to delegate the search to the police alone because they are unfamiliar with the area and do not know which objects in the facility would look unusual or out of place. The most effective search is possible when all employees are calmly told about the bomb threat and the reason for the search and are then asked to check their familiar areas for suspicious objects. Teams should be organized to search common areas. A search team leader should be designated and a noti-

fication protocol developed to report search results to the facilities manager. A plan should be developed to designate who is responsible for searching a specific area—for example, security will search restrooms and outside areas, while facilities staff will search LAN and electrical rooms.

The objective of the search activity is to search for and report suspicious objects. There are several points to be stressed within search plans:

- The search should be systematic (divide the facility into search areas), it should be thorough, and it should be done calmly. It should be done by company personnel. Identify the areas that are most accessible to outsiders and the areas that are most vulnerable; search them first.
- When searching a room, the room should first be searched from floor to waist height, then from waist height to eye level, and finally from eye level to ceiling. If the room has a false ceiling, the false ceiling should also be inspected and searched.
- **Nobody should move, touch, or jar any suspicious object or anything attached to it. The removal or disarming of a bomb must be left to law enforcement professionals.**

No Bomb Found

If no bomb (or suspicious object) is found, the facilities manager should advise employees, the police, and local management and return the operation to normal activity.

Suspicious Object Found

If a suspicious object is found, the search team coordinator and the facilities manager should do the following:

- Stress again to personnel not to touch or move the object.
- Evacuate personnel from the surrounding area.
- Prevent re-entering of the evacuated area.
- Inform the police who will take charge of getting the object deactivated and removed.
- After the object has been removed, finish searching to ensure that no other bombs have been placed.

Bomb Explosion

If there is a bomb explosion, the facilities or security manager should take these steps:

- Determine if there are any injuries and attend to them immediately.
- Evacuate the surrounding area.
- Ensure no one goes near the scene of the explosion except to remove the injured.
- Control access to the area as other bombs may have been set to detonate at intervals.
- Advise police who will take charge of the situation.
- Initiate the on-site emergency plan if fire fighting or other medical response becomes necessary.

After-Action Plan

An after-action report, including incorporation of lessons learned, should be prepared immediately after resolution of the event.

Sample Bomb Threat Telephone Card

A card like this can be printed on narrow paper and placed under telephones to help employees who receive bomb threats.

Time Call Received:

Date:

Exact wording of bomb threat:

Listen—do not interrupt! After caller stops volunteering information, ask these questions, trying to keep the caller on the line:

1. When is the bomb going to explode?
2. Where is the bomb right now?
3. What does the bomb look like?
4. What kind of bomb is it?
5. What will cause the bomb to explode?
6. Did you place the bomb?
7. Why?
8. What is your address?
9. What is your name?

Record the following information:
Sex of caller:
Age:
Length of call:

Telephone number at which call was received:

Caller's voice (check the appropriate descriptors):

Calm	Disguised
Angry	Soft
Excited	Loud
Slow	Laughter
Rapid	Crying
Distinct	Normal
Ragged	Whispered
Cracking	Deep Breathing
Nasal	Accent
Stutter	Clearing Throat
Lisp	Slurred
Rasp	Deep

Familiar—If familiar, who does it sound like?

Background sounds (check the appropriate descriptors):

Street Noises	Factory Machinery	Voices
Crockery	Animal Noises	Clear
PA System	Static	Music
House Noises	Long Distance	Local
Motor	Office Machinery	Booth

Other: _____

Bomb threat language (check the appropriate descriptors):

Well-spoken (educated)	Incoherent	Foul
Irrational	Taped	Threat
Read		

Your Remarks:

Your name:
Your position:

Report the call immediately to:

4. Sample Pre-employment Screening Policy

It is standard [Company Name] practice to require pre-employment background screening, as specified below, as a means of verifying applicant data prior to hire. This standard applies to regular and non-regular employments, including rehires where the separation period is more than 30 days. Pre-employment background screening is required for all rehires into designated positions regardless of the duration of the separation period.

It is intended that background checks will be made after reaching a decision to offer employment following the usual candidate review process.

Failures to disclose and discrepancies between the employment application and a background report will be reviewed and evaluated by HR. HR will consult with Security and Labor/Employment Law as appropriate. Any additional investigation will be conducted by [Company Name] Security or the company's designated third-party background screening agency. Criteria for evaluating background reports are set out below, following the background screening matrix. Copies of all investigative reports should be retained in the candidate's file.

Any decision on employment, or on discipline or termination of a current employee, as a result of information generated by the background checks should be reviewed for consistency and endorsed by [Company Name] Recruiting & Employment, Security, and Labor/Employment Law.

Waiver Provision

Hiring an individual prior to completion of pre-employment background screening is discouraged. However, where it is deemed necessary due to business necessity, approval may be authorized by the hiring organization's senior management following endorsement by Security and HR. In such cases, the individual's employment will be conditioned on completion of the pre-employment background screening and evaluation process. No exceptions to pre-employment background screening involving designated positions are permitted.

In considering conditional employment arrangements due to business necessity (typically restricted to executives), organizations should balance operational needs against other considerations/exposures to the company. Because candidate disqualifications due to background problems occur regularly, at least the following issues should be considered before early hire is approved:

1. In almost all cases, if there is a problem, it will be impractical to attempt to recover relocation costs, e.g., home search, new hire loan, home sale/purchase, home finding/interim living lump sum, moving expenses, relocation allowance/miscellaneous expense payment, etc., as well as salary advances and training costs.
2. Individuals may quit their current job, remove children from established schools, etc. to accept [Company Name] employment, increasing the possibility the individual will challenge a decision to revoke the offer.
3. The above factors put pressure on the objectivity of the decision-making process when there is an issue with the background report.
4. The removal of the employee from the workplace may disrupt the workplace and harm the morale of other employees.

PRE-EMPLOYMENT BACKGROUND SCREENING MATRIX

Types	Identification	Employment History	Education	Criminal Record	Motor Vehicle Record	Credit History	Military	Prof. Accred.	Pre-Place Medical Assess	INS Form I-9
New Regular Hires	X	X	X	X	X	X	X	X	X	X
Contractors and Vendors	X	-	-	X	X	X	-	-	X	X

Note: Shaded areas represent services to be purchased from third-party vendor.

Employment Application and Background Report Principles

Any intentional misrepresentation or failure to disclose information on the employment application should result in immediate revocation of the employment offer, or termination of employment if the applicant has been employed.

Any felony, misdemeanor, or other offense (including attempt or conspiracy) that is relevant to the work to be performed by an applicant or to the presence of the individual on company premises, that is either disclosed by an applicant or discovered in a background check should result in immediate revocation of the employment offer, or termination of employment if the applicant has been employed. Factors such as commission of the offense when a youth and very old convictions may, in some circumstances, work against relevance and a decision to revoke or terminate. Even if an applicant has not been formally convicted of a crime or offense (for example, in the case of a "deferred adjudication" [except where consideration is prohibited by law] or an unresolved charge or indictment), if investigation determines that the applicant engaged in conduct of the type prohibited, the offer should be revoked or employment terminated, as set out above. The types of crimes and offenses that are usually found to be relevant include, but are not limited to, the following:

- Theft (e.g., robbery, theft, burglary, hot checks, etc.)
- Fraud or embezzlement
- Industrial espionage or trade secret theft
- Physical violence, such as assault, battery, or homicide
- Sexual crimes
- Sale, distribution, or possession of illegal substances
- Weapons or contraband-related offenses
- DWI, DUI, public intoxication, or other alcohol or drug offenses (always relevant for designated positions and security drivers)

5. Sample Workplace Violence Policy

Adapted from "Combating Workplace Violence" by the Defense Personnel Security Research Center for the International Association of Chiefs of Police (IACP).

Nothing is more important to (Company Name) than the safety and security of its employees. Threats, threatening behavior, or acts of violence against employees, visitors, guests, or other individuals by anyone on (Company Name) property will not be tolerated. Violations of this policy will lead to disciplinary action, which may include dismissal, arrest, and prosecution.

Any person who makes substantial threats, exhibits threatening behavior, or engages in violent acts on (Company Name) property shall be removed from the premises as quickly as safety permits, and shall remain off (Company Name) premises pending the outcome of an investigation. (Company Name) will initiate an appropriate response. This response may include, but is not limited to, suspension or termination of any business relationship, reassignment of job duties, suspension or termination of employment, or criminal prosecution of the person or persons involved.

No existing (Company Name) policy, practice, or procedure should be interpreted to prohibit decisions designed to prevent a threat from being carried out, a violent act from occurring, or a life-threatening situation from developing.

All (Company Name) personnel are responsible for notifying the management representative designated below of any threats they have witnessed or received and any threats that they have been told another person has witnessed or received. Even without an actual threat, personnel should report any behavior they have witnessed which they regard as threatening or violent when that behavior is job-related, might be carried out on a company-controlled site, or is connected to company employment. Employees are responsible for making this report regardless of the relationship between the individual who initiated the threat or threatening behavior and the person or persons who were threatened or were the focus of the threatening behavior. If the designated management representative is not available, personnel should report the threat to their supervisor or another member of the management team.

All individuals who apply for or obtain a protective or restraining order that lists company locations as protected areas must provide to the designated management representative a copy of the petition and declarations used to seek the order, a copy of any temporary protective or restraining order granted, and a copy of any protective or restraining order that is made permanent.

(Company Name) understands the sensitivity of the information requested and has developed confidentiality procedures that recognize and respect the privacy of reporting employees.

The designated management representative is:

Name:_____

Title:_____

Department:_____

Telephone:_____

Location:_____

6. Sample Employee Misconduct Policy

These rules address serious acts of misconduct obviously contrary to the ability to maintain a safe, respectful, orderly, and productive workplace. The actions and behaviors listed below will not be tolerated. This means all such acts will be treated as extremely serious violations of the rules of conduct for which discharge will be the first consideration. The list of items below is not intended to represent a complete list of unacceptable conduct. There may be other acts of misconduct that result in the same consequences.

1. Violations of safety rules, practices or policies
2. Dishonesty
3. Engaging in hostile, abusive, threatening, or disrespectful behavior while engaged in activities on behalf of the company, including physical or mental intimidation, threats, or sexual or other forms of harassment
4. Use of abusive, threatening, provocative, or inflammatory language or gestures
5. Receiving or attempting to receive pay under fraudulent circumstances or any other attempts to defraud the company
6. Falsification of records, data documents, or other information including giving false or incomplete information during employment or when applying for employment, or in connection with management investigations
7. Engaging in a fight in the workplace or on site property or in activity that could provoke fighting
8. Use or possession of weapons, ammunition, explosives, or fireworks on site property or in the workplace
9. Use, sale, distribution, manufacture, dispensing, or possession of drugs or alcohol in the workplace
10. While in the workplace, “presence in the body” of alcohol or drugs taken for non-medical reasons
11. Insubordination, including deliberate refusal to comply with reasonable requests or instructions
12. Absence from work without notice or authorization from supervision, unless the cause of absence prevents giving notice
13. Conduct which violates common decency or morality
14. Use of company electronic communications resources for non-business purposes, including unauthorized access to the Internet or access to websites that are inconsistent with company policies, ethics, values, and business practices
15. Horseplay or malicious mischief
16. Using or divulging, without permission, confidential information such as trade secrets, process know-how, personnel data, salary information, business data, etc., regardless of whether the information is taken wrongfully by the employee or merely passed on by the employee
17. Theft, unauthorized possession, removal, or attempted removal of company property or property belonging to employees, contractors, vendors, or visitors
18. Sleeping on the job
19. Intentional damage to company, employee, contractor, or vendor property
20. Bringing “strike anywhere” matches on-site, or having any type of match, cigarette lighter, or flame-producing device in restricted areas
21. Smoking except in designated smoking areas

7. Sample General Weapons Policy

In keeping with [Company Name]'s intent to provide a safe and secure work environment for its employees, a "no weapons" policy has been instituted. No weapons of any sort (knife with blade over 2½ inches long, handgun, rifle, shotgun, or other weapons originally designed, made, or intended to fire a projectile by means of an explosion from one or more barrels) are permitted on [Company Name]'s premises. This includes parking lots, leased buildings, leased vehicles, and recreation areas before, during, and after normal business hours. This policy also applies when associates are conducting company business, whether or not on company premises. The sole exceptions apply to military or law enforcement personnel in the performance of their duties and armored car escorts making pickups and deliveries (but side arms are to be holstered inside a facility).

8. Sample Policy on Drug and Alcohol Use

[Company name] is committed to a safe, healthy, and productive workplace for all employees. The company recognizes that alcohol, drug, or other substance abuse by employees will impair their ability to perform properly and will have serious adverse effects on the safety, efficiency, and productivity of other employees and the company as a whole. The misuse of legitimate drugs, or the use, possession, distribution, or sale of illicit or unprescribed controlled drugs on company business or premises, is strictly prohibited and is grounds for termination. Possession, use, distribution, or sale of alcoholic beverages on company premises is not allowed without prior approval of appropriate senior management. Being unfit for work because of use of drugs or alcohol is strictly prohibited and is grounds for termination of employment. While this policy refers specifically to alcohol and drugs, it is intended to apply to all forms of substance abuse.

The company recognizes alcohol or drug dependency as a treatable condition. Employees who suspect that they have an alcohol or drug dependency are encouraged to seek advice and to follow appropriate treatment promptly before it results in job performance problems. Employee health advisory program or medical professional staff will advise and assist in securing treatment. Those employees who follow approved treatment will receive disability benefits in accordance with the provisions of established benefit plans and medical insurance coverage consistent with existing plans.

No employee with alcohol or drug dependency will be terminated due to the request for help in overcoming that dependency or because of involvement in a rehabilitation effort. However, an employee who has had or is found to have a substance abuse problem will not be permitted to work in designated positions identified by management as being critical to the safety and well-being of employees, the public, or the company. Any employee returning from rehabilitation will be required to participate in a company-approved aftercare program. If an employee violates provisions of the employee Alcohol and Drug Use Policy, appropriate disciplinary action will be taken. Such action cannot be avoided by a request at that time for treatment or rehabilitation. If an employee suffering from alcohol or drug dependency refuses rehabilitation or fails to respond to treatment or fails to meet satisfactory standards of effective work performance, appropriate disciplinary action, up to and including termination, will be taken. This policy does not require and should not result in any special regulations, privileges, or exemptions from normal job performance requirements.

The company may conduct unannounced searches for drugs and alcohol on owned or controlled property. The company may also require employees to submit to medical evaluation or alcohol and drug testing where cause exists to suspect alcohol or drug use. Unannounced periodic or random testing will be conducted when an employee has had a substance abuse problem or is working in a designated position identified by management, a position where testing is required by law, or a specified executive position. A positive test result or refusal to submit to a drug or alcohol test is grounds for disciplinary action, including termination.

Contractor, common carrier, and vendor personnel are also covered by paragraph one and the search provisions of paragraph four of this policy. Those who violate the policy will be removed from company premises and may be denied future entry.

In addition to the above policy, it is a requirement of the company that all applicants accepting offers of regular employment must pass a drug test.

9. Compact, Unified Security Policy and Procedures: Sample 1

It is important that management state the security behavior expected while persons are on company property or performing duties directly related to work requirements. This may best be done by the issuance of a written policy, which articulates expectations and compliance criteria. Procedures to comply with the policy should also be provided.

Access Control:

Policy: It is the policy of [Company Name] that access to the facility be limited to those who have been granted authorization for access.

Procedures: The property boundary will be clearly defined. Signage will be used to direct entrants to the appropriate entry point for processing onto the facility. Management will define the process for granting authorization for access to an individual. This may include verification of safety briefings and utilization of personal protection equipment. Employees, visitors, and contractors will log into and out of the facility, when entering or exiting the facility after being granted access authorization.

Pre-employment Screening

Policy: It is the policy of [Company Name] that pre-employment screening will be conducted on candidates for employment.

Procedures: Human Resources will contract with a third-party provider approved by Corporate Human Resources to conduct such screens.

Workplace Violence

Policy: [Company Name] has "zero tolerance" for any incident of violence in the workplace, whether it be physical violence, verbal abuse, willful destruction of company property, or any form of intimidation that affects the morale of the workforce. Such acts may be cause for counseling, reprimand, or even termination of employment. Alleged incidents will be investigated and sanctions exercised when warranted.

Procedures: Incidents of violence shall be reported to management immediately. Management will take appropriate action to defuse an ongoing confrontation and to gather evidence for investigation. Those involved in the incident shall be suspended from work, pending conclusion of the investigation. After consideration of the facts, management will adjudicate the incident.

Employees victimized by violence, who obtain court-issued restraining orders, shall notify management immediately and provide copies of documentation. Management will notify law enforcement of any violations.

Drug and Alcohol Abuse

Policy: [Company Name] has a corporate policy on this subject.

Procedures: Local management should publicize the policy to all employees and, as necessary, supplement the policy to reflect local conditions and requirements. NOTE: Local management can only increase the severity of the policy, not reduce any conditions of the corporate policy.

Protection of Information

Policy: It is the policy of [Company Name] that all company information—classified confidential, internal, or external—be secured from unauthorized disclosure or misuse.

Procedures: Management will define information to be safeguarded. Information will be disclosed on a limited basis and will be stored in a locked desk, file cabinet, or safe when not in use. Employees, visitors, vendors, and contractors will be required to sign statements of confidentiality before being granted access to the facility.

Weapons on Company Property

Policy: [Company Name] has a corporate policy on this subject.

Procedures: Management should ensure that anyone entering a [Company Name] facility is made aware of the restriction of weapons on company property. Exceptions to the policy are available based on specific needs. The policy and procedures should be supplemented at the local level to ensure compliance and enforcement.

Incident Reporting

Policy: It is the policy of [Company Name] that security incidents be reported immediately to Corporate Security.

Procedures: Security incidents should be reported to Corporate Security by calling [phone number]. This will be followed by the submission of an incident reporting form. If security guards are employed, the security post orders should include a requirement that the officer call [phone number] about all emergency incidents.

10. Compact, Unified Security Policy and Procedures: Sample 2

1.0 APPLICABILITY: This policy shall apply to all company facilities.

2.0 PURPOSE: To require that minimum site security provisions be implemented to prevent harm to individuals, to avoid business interruption, and to prevent loss of property and information, due to theft, vandalism, violence, illegal and disruptive activities by extremist groups, and other criminal acts against the company.

3.0 POLICY: Each company location shall implement a site security program. The program will be developed considering the following potential sources of loss or disruption:

- 3.1 Theft, vandalism, and break-ins, considering both internal and external threats
- 3.2 Theft of confidential business information
- 3.3 Sabotage of equipment, utilities, and records; product contamination and tampering
- 3.4 Bomb threats
- 3.5 Demonstrators disrupting plant access and operations
- 3.6 Workplace violence and assaults

4.0 POLICY: Each company location shall designate an employee as the site security coordinator. This person shall be responsible for performing the following security management functions:

- 4.1 Preparing and implementing a site security plan consistent with the requirements contained herein
- 4.2 Establishing relationships with law enforcement agencies
- 4.3 Developing and managing incident reporting systems and conducting investigations of breaches of company security policy
- 4.4 Developing methods to increase employees' security awareness
- 4.5 Working with the site emergency coordinator to address security issues in emergency and crisis management planning and execution
- 4.6 Periodically reassessing the site's security program

5.0 POLICY: The security measures at each site shall include the following provisions:

- 5.1 Access control for people and vehicles into production areas, warehouses, utility facilities, and offices that contain business information that needs to be protected ("controlled areas")
  - 5.1.1 Signs to direct all visitors and vehicles to the appropriate entry points
  - 5.1.2 A system to verify visitors (any non-employee) and vehicles prior to entering company premises, along with safety and security briefing for all visitors
  - 5.1.3 For non-employees, mandatory sign-in for access to controlled areas for at least the first visit (policy on escorting visitors during subsequent visits to be developed by the location)
  - 5.1.4 Identifying badge for all visitors, along with requirement to wear the badge so it is visible

5.1.5 Controlled areas to be provided with physical barriers capable of keeping unauthorized people and vehicles out, except through designated entrance points (barriers shall not impede emergency egress from facilities)

5.1.6 Access points to controlled areas placed so that receptionist has a clear and remote view of visitors and vehicles approaching the facility

5.2 Perimeter protection (such as fences, solid exterior walls, gates to block vehicle traffic, and perimeter lighting) around controlled areas

5.3 Off-hours protection for controlled areas, such as remotely supervised intrusion alarms or a contract security guard service touring the facility regularly

5.4 Back-up power systems for controlled areas where operations are critical and for intrusion alarm and safety systems

6.0 POLICY: For employee security issues, refer to existing HR policies on the following subjects:

- Pre-employment screening
- Employee termination
- HR services
- "Zero tolerance" for violence
- Prohibition of weapons on company facilities, including parking lots
- Confidential business information
- Internal incident reporting systems
- Referring illegal or criminal activities to law enforcement