IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

ChemLock: Policies, Plans, and Procedures Security Goal

Developing a Security Plan

CHEMLOCK
Know your chemicals.
Lock in your security posture.

The Cybersecurity and Infrastructure Security Agency (CISA) encourages facilities with dangerous chemicals to develop a holistic, customized, site-specific security plan that mitigates risk and enhances chemical security at the facility. To assist your facility in developing a security plan, the ChemLock program presents five security goals to consider as you evaluate and implement security measures tailored to your facility's unique circumstances and business model. This fact sheet provides an overview of the Policies, Plans, and Procedures security goal.

Policies, Plans, and Procedures Security Goal

Policies, plans, and procedures ensure you have the capability to manage your facility security plan, including the development and implementation of policies, procedures, and other processes that support security plan implementation and oversight. Your facility's security plan cannot be effective without combining cyber and physical security measures with written procedures to help you execute all aspects of the security plan.

Examples of Policies, Plans, and Procedures

Examples of policies, plans, and procedures include maintenance, inspection, and testing of security equipment; a security awareness and training program; background checks on personnel; an insider threat program; a visitor escort policy; processes for incident reporting and investigations; and the establishment of roles and responsibilities for facility personnel and recordkeeping policies.

Policies, plans, and procedures will vary by the needs of the facility, but generally include:

1. **Maintenance, inspection, and testing of security equipment.** Regular maintenance, inspection, tests, repairs, and improvements to the security, safety, and communications systems increases the reliability of such systems and will improve response time.
2. **Security awareness and training program.** A security awareness and training program (SATP) is a predefined and documented set of scheduled activities. This can include training, exercises, drills, tests, and joint initiatives that focus on relevant security-related issues for your facility and enhance the overall security awareness of all facility personnel.
3. **Background checks on personnel.** Background checks can significantly improve your facility's ability to deter, detect, and defend against insider threats or other covert attacks. Checks to consider include employment history, educational history, criminal history, and credentials.
4. **Insider threat program.** Current or former employees with access to and knowledge of your organization's internal policies and procedures can intentionally use that access to harm your organization. Carefully consider scenarios for insider threat while developing all areas of your security plan and what could happen if these areas were compromised.

5. **Visitor escort policy.** Identification and control mechanisms for visitors can help mitigate the risk posed to your facility by visitors.
6. **Processes for incident reporting and investigations.** Your facility should have an incident reporting and investigation program so that all significant security incidents are promptly and adequately reported to the appropriate facility personnel, local law enforcement entities, and CISA, as applicable, and to ensure that investigations are thorough in order to reveal vulnerabilities and identify corrective actions.
7. **Officials, organization, and records.** To establish and reinforce a security culture, maintaining a security organization so employees understand their roles and responsibilities as they relate to security is an imperative. In addition, the establishment of a records management program ensures that your organization is following established policies and programs and allows for a comprehensive audit program.

Considerations for Policies, Plans, and Procedures

When developing and implementing policies, plans, and procedures, your facility should account for its operational constraints and business needs. For example, a visitor escort policy will look very different at a retailer when compared to a manufacturing facility. Similarly, maintenance, inspection, and testing of security equipment will vary based on the detection, delay, cyber, and response security measures implemented at the facility.

It is important to ensure that all appropriate facility and third-party personnel are included in the development and implementation of the policies, plans, and procedures. Appropriate personnel should also be thoroughly trained in the policies, plans, and procedures to ensure awareness and familiarity. Policies, plans, and procedures should be tested periodically via exercises or drills so that they remain relevant and up to date.

Security-in-Depth

An optimal security plan typically involves the use of multiple security measures that provide layers of security (also known as security-in-depth). Complementary layers of security measures not only ensure that your critical assets are secured against different kinds of security threats, but also provide redundancy in case one security measure fails or is compromised by a nefarious actor. Policies, plans, and procedures are part of security-in-depth and are critical to any security plan.

CISA Security Resources

- ChemLock: cisa.gov/chemlock
- ChemLock: Secure Your Chemicals: cisa.gov/chemlock-security-plan
- ChemLock Exercises: cisa.gov/chemlock-exercises

Next Steps

Here are some questions you can use to evaluate your facility's policies, plans, and procedures:

- How often is your security equipment inspected and tested?
- What kind of security awareness and training program has been established?
- How are background checks conducted for new and current personnel?
- Is there an established insider threat program?
- Is there an established reporting process for suspicious activity?
- Do all personnel know who to contact in the event of a security incident at your facility?
- What processes have been implemented for keeping records of policies, plans, and procedures?
- How often are audits or exercises conducted to ensure that policies, plans, and procedures are up to date?