ChemLock: Conducting a Chemical Security Self-Assessment

Periodically reviewing and assessing the security measures in a facility’s security plan is a critical component in maintaining an effective security plan. This document serves as a template to help facilities conduct a self-assessment. For more information on developing a facility chemical security plan, visit [cisa.gov/chemlock-security-plan](https://www.cisa.gov/chemlock-security-plan).

CISA encourages facilities to review their security plan on an annual basis as personnel, processes, policies, and procedures can change over time. A facility security plan assessment should:

* Ensure the plan meets its goals and is effective.
* Confirm that all the information is up to date.
* Identify security gaps and corresponding mitigation measures.
* Review the implementation of additional planned measures.
* Incorporate any changes as necessary to existing security measures.
* Identify and remove obsolete measures that are no longer necessary.
* Review relevant policies, plans, and procedures, such as roles and responsibilities, password procedures, reporting procedures for suspicious activity and security incidents, and response measures to an incident or hazard.

The checklist below uses five security goals to help facility personnel identify gaps in security measures so that any vulnerabilities can be addressed. If a security gap is found, the facility can identify steps and develop timelines to resolve those identified gaps. The ChemLock program also offers on-site assessments and assistance to help facilities assess security measures and identify any security gaps. For more information, visit [cisa.gov/chemlock-assessments](https://www.cisa.gov/resources-tools/programs/chemlock/chemlock-assessments).

[FACILITY NAME] Chemical Security Plan Assessment Template

Facility Name:   
Facility Address:   
Facility Point of Contact (POC):   
Facility POC Phone:   
Facility POC Email:   
Facility Assessed By:   
Assessment Date:

This table can serve as a baseline from which to begin an assessment and can be customized to fit the needs and unique circumstances of your facility. If you would like assistance conducting a facility security assessment, request a ChemLock service at [cisa.gov/chemlock-assessments](https://www.cisa.gov/resources-tools/programs/chemlock/chemlock-assessments).

For more information on the five ChemLock security goals, visit [cisa.gov/chemlock-security-goals](https://www.cisa.gov/resources-tools/programs/chemlock/security-goals).

| **Security Plan Item** | **Verified (Yes/No)** | **Comments** |
| --- | --- | --- |
| **Review and Update Contact Information** |  |  |
| Facility Contact Information |  |  |
| Responder and Other Contact Information |  |  |
| **Critical Asset Identification** |  |  |
| Chemical and Asset Name |  |  |
| Location |  |  |
| Use |  |  |
| **Detection** |  |  |
| Intrusion Detection System |  |  |
| Camera System |  |  |
| Employees and On-Site Personnel |  |  |
| Security Lighting |  |  |
| Chemical Product Inventory |  |  |
| Additional Detection Security Measures |  |  |
| **Delay** |  |  |
| Perimeter and Asset Barriers |  |  |
| Physical Locking Mechanism |  |  |
| Access Control |  |  |
| Inspection and Screening |  |  |
| Shipping and Receiving Procedures |  |  |
| Additional Delay Security Measures |  |  |
| **Response** |  |  |
| Emergency Response Procedures/Crisis Management Plan |  |  |
| Outreach Programs |  |  |
| Security Plans for Elevated Threats |  |  |
| Additional Response Security Measures |  |  |
| **Cyber** |  |  |
| Cybersecurity Measures |  |  |
| Cybersecurity Policies and Procedures |  |  |
| Access Control and Password Management |  |  |
| Cybersecurity Employee Training and Process |  |  |
| Controls, Monitoring, Response, and Reporting |  |  |
| Disaster Recovery and Business Continuity |  |  |
| Additional Cybersecurity Measures |  |  |
| **Policies, Plans, and Procedures** |  |  |
| Maintenance, Inspection, and Testing of Security Equipment Program |  |  |
| Security Awareness and Training Program |  |  |
| Employee Background Checks |  |  |
| Insider Threat Program |  |  |
| Visitor Escort Policy |  |  |
| Incident Reporting and Investigations Policy |  |  |
| Officials, Organizations, and Records Policy |  |  |
| Additional Policies, Plans, and Procedures |  |  |