Facility Chemical Security Plan

[Name of Facility]

[Updated Month Year]

This document contains interactive components within the MS Word application that are inherently not accessible to certain individuals. To request a fully accessible version of this facility security plan template, please email ChemLock@cisa.dhs.gov.

[Insert organization logo on the cover page as desired.]

Instructions

Understanding security principles is valuable, but without a facility security plan that implements specific security measures to meet those security principles, facilities may be unnecessarily exposing themselves to risk. The Cybersecurity and Infrastructure Security Agency (CISA) encourages facilities with dangerous chemicals to use this facility security plan template to develop a holistic, customized, site-specific security plan that mitigates risk and ensures chemical security at your facility.

Additional information and guidance on developing a facility security plan is available in ChemLock: Secure Your Chemicals on the [ChemLock Security Plan webpage.](https://www.cisa.gov/chemlock-security-plan)

In combination with “Part 1: Security Goals” of the ChemLock: Secure Your Chemicals guidance document, this security plan template helps facilities evaluate how dangerous chemicals are currently secured, identify gaps in security, and, ultimately, put plans in place to meet the various security goals described in ChemLock: Secure Your Chemicals ([cisa.gov/chemlock-security-plan](https://www.cisa.gov/chemlock-security-plan)):

* Critical asset identification (i.e., location, packaging, and other pertinent logistical information for onsite chemicals)
* Risk Management
* Detection security measures
* Delay security measures
* Response security measures
* Cybersecurity measures
* Policies, plans, and procedures to implement specific security measures

This plan should be developed with input from the facility’s onsite security, safety, and logistical professionals to encompass all components of a security plan. Once a plan has been devised, facilities are encouraged to train all personnel on the plan and to establish an annual audit of the plan to ensure ongoing effectiveness, keeping in mind that security measures may need to change. It is also important to ensure contact information is identified and updated in the plan for local law enforcement and fire departments, as well as regulatory agencies, should emergencies arise.

Facilities may delete these instruction pages from your facility security plan document.

Since there are a multitude of facility types that use potentially dangerous chemicals, aspects of this template security plan may not be applicable to all facilities.

If you have any questions or feedback pertaining to the security goals, aspects of this facility security plan, or other chemical security related topics, please email ChemLock@cisa.dhs.gov. To request CISA’s chemical security expertise in helping to develop a facility security plan, please fill out the [ChemLock Services Request Form](https://www.surveymonkey.com/r/T9ZTBRT).

Revisions

| Revision Version | Date Finalized | Effective Date | Authorized By |
| --- | --- | --- | --- |
| Ex. v1.0 | January 21, 2022 | February 1, 2022 | Facility Security Officer John Doe |
|  |  |  |  |

Contact Information

Facility Contact Information

|  |  |
| --- | --- |
| Facility Name: |  |
| Address: |  |
| Facility’s Primary Contact – Name: |  |
| Facility’s Primary Contact – Phone/Email: |  |
| Facility Security Officer: |  |
| Facility Security Officer Phone/Email: |  |
| Cybersecurity Officer: |  |
| Cybersecurity Officer Phone/Email: |  |
| Hours of Operation: |  |
| Special Hours or Closures (Describe): |  |

Other Contact Information

|  |  |
| --- | --- |
| Local Law Enforcement: |  |
| Local Fire Department or First Responders: |  |
| County Emergency Management Agency Official: |  |
| City/Town/Locality Emergency Management Agency Official: |  |
| County Public Health Official: |  |
| City/Town/Locality Public Health Official: |  |
| Local Emergency Planning Committee (LEPC) Chair: |  |
| LEPC Vice-Chair: |  |
| Cybersecurity and Infrastructure Security Agency (CISA) Chemical Security Personnel: |  |
| Federal Bureau of Investigation (FBI) Weapons of Mass Destruction (WMD) Coordinator: |  |

Critical Asset Identification

Identifying the dangerous chemicals at your facility is the first step in determining what you need to protect and how you will protect them from threats.

Directions

* For each chemical, describe the location at your site and how it is used.
* Consider the inclusion of maps or plot plans in your security plan to help your facility personnel and emergency responders quickly identify the locations of dangerous chemicals.

Critical Assets

| Chemical | Critical Asset Name | Location | Use (i.e., Ship, Sell, Manufacture, Receive) |
| --- | --- | --- | --- |
| Ex. Chlorine | Chlorine Storage Cage | Warehouse Building 1 | Receive |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Notes

Click or tap here to enter text.

Detection

Detection includes the capability to identify potential attacks or indicators of an attack—such as the theft, release, or sabotage of your chemicals—and to communicate that information, as appropriate.

Directions

* Assess how your facility currently detects unauthorized access or suspicious activities.
* When you have identified the current security measures, compare them to the security principles laid out in Part 1, Section 3, Detection.
* Use this portion of the security plan to ensure each security measure is properly implemented and confirm whether it covers the chemical asset area.
* Identify any gaps in detection capabilities and any additional security measures that may be necessary to close those gaps.
* Develop a plan to implement any additional security measures.
* Consider your facility’s operational hours when conducting this assessment and assigning security measures.

Notes

Click or tap here to enter text.

Detection Security Measures

1. Intrusion detection system (IDS): Yes [ ]  No [ ]
	1. Areas and critical assets that the IDS covers (Use chemical asset names identified above and nomenclature for your facility):
	Click or tap here to enter text.
	2. IDS monitoring by: Click or tap here to enter text.
	3. IDS response by: Click or tap here to enter text.
	4. System backup power supply: Yes [ ]  No [ ]
		1. Click or tap here to enter text. hours of backup power available
		2. If no backup power, are there other compensatory measures?
		Yes [ ]  No [ ]
		If yes, describe: Click or tap here to enter text.
	5. Hours of active IDS monitoring: Click or tap here to enter text.
	6. Types of sensors (Select all that apply):
	[ ]  Fence-mounted sensors
	[ ]  Wall-mounted sensors
	[ ]  Window-mounted sensors
	[ ]  Volumetric sensors
	[ ]  Beam sensors
	[ ]  Gate/door sensors
	[ ]  Counter-UAS/object-detecting sensors
	[ ]  Other (Describe): Click or tap here to enter text.
2. Camera system: Yes [ ]  No [ ]
	1. Areas and critical assets that the camera system covers (Use chemical asset names identified above and nomenclature for your facility):
	Click or tap here to enter text.
	2. Camera system monitored by: Click or tap here to enter text.
	3. Camera system response by: Click or tap here to enter text.
	4. Camera system backup power supply: Yes [ ]  No [ ]
		1. Click or tap here to enter text. hours of backup power available
		2. If no backup power, are there other compensatory measures?
		Yes [ ]  No [ ]
		If yes, describe: Click or tap here to enter text.
	5. Camera system includes video motion detection: Yes [ ]  No [ ]
	6. Camera system is integrated with IDS: Yes [ ]  No [ ]
	If yes, describe: Click or tap here to enter text.
3. Employees and onsite security personnel
	1. The facility has onsite security personnel: Yes [ ]  No [ ]
		1. Hours security personnel are onsite: Click or tap here to enter text.
		2. Locations where security personnel are posted (Use chemical asset names identified above and nomenclature for your facility):
		Click or tap here to enter text.
		3. Frequency of roving patrol: Click or tap here to enter text.
	2. Employee presence
		1. Hours employees are onsite: Click or tap here to enter text.
		2. Locations with employee presence (Use chemical asset names identified above and nomenclature for your facility):
		Click or tap here to enter text.
		3. Employee training includes:
			1. Security awareness training: Yes [ ]  No [ ]
			2. Personnel detection training: Yes [ ]  No [ ]
4. Security lighting
	1. There is sufficient lighting on asset areas for security equipment (i.e., camera systems, fencing, IDS, etc.): Yes [ ]  No [ ]
	2. Lighting coverage areas:
		1. Interior (Describe): Click or tap here to enter text.
		2. Exterior (Describe): Click or tap here to enter text.
	3. Security lighting backup power supply: Yes [ ]  No [ ]
		1. Click or tap here to enter text. hours of backup power available
		2. If no backup power, are there other compensatory measures?
		Yes [ ]  No [ ]
		If yes, describe: Click or tap here to enter text.
5. Chemical product inventory
	1. Frequency of inventory: Click or tap here to enter text.
	2. Inventory conducted by: Click or tap here to enter text.
	3. Inventory management system, if applicable: Click or tap here to enter text.
	4. Discrepancies in inventory are reported to: Click or tap here to enter text.

Additional Security Measures

If gaps in detection capabilities were identified for any of the chemical assets listed in this section of this security plan, consider what additional security measures might be needed to close the identified gap. In this portion, identify specific security measures that your facility will plan to implement in the future to ensure detection.

Tip: Include a timeline and point of contact responsible to ensure accountability and project completion.

Click or tap here to enter text.

Delay

Delay means physically limiting access to the facility and/or asset(s) to reduce the likelihood of an adversary successfully breaching the facility perimeter and/or asset(s) or using the area immediately outside of the facility’s perimeter to launch an attack.

Complete perimeter security is rarely attained through the deployment of a single security barrier; rather, an optimal security solution typically involves the use of multiple protective measures that provide layers of security. Layering of security measures can be achieved by incorporating different types of security measures (e.g., integrating physical protective measures—such as barriers, lighting, and electronic security systems—with procedural security measures—such as procedures guiding how security personnel should respond to an incident). When developing a layered security approach, facilities should consider how to use existing facility and natural features or other technologies applicable to the facility’s circumstances to meet the performance objectives at a reduced cost.

Directions

* Assess how your facility currently provides delay capabilities and prevents unauthorized access.
* When you have identified the current security measures, compare them to the security principles laid out in Part 1, Section 4, Delay of ChemLock: Secure Your Chemicals ([cisa.gov/chemlock-security-plan](https://www.cisa.gov/chemlock-security-plan)).
* Use this portion of the security plan to ensure each security measure is properly implemented and confirm whether it covers the chemical asset area.
* Identify any gaps in delay capabilities and any additional security measures that may be necessary to close those gaps.
* Develop a plan to implement any additional security measures.
* Consider your facility’s operational hours when conducting this assessment and assigning security measures.

Notes

Click or tap here to enter text.

Delay Security Measures

1. Perimeter and asset barriers
	1. Defined perimeter and asset characteristics
		1. Type of perimeter and asset barriers (Use chemical asset names identified above and nomenclature for your facility) (Select all that apply):

| Perimeter/Asset Name | Fence | Wall | Bollards | Berms | Ditches | Jersey Barriers | Other (Describe) |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Ex. West perimeter | X |  |  |  | X |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

* + 1. No trespassing/restricted area/private property signage posted:
		Yes [ ]  No [ ]
		2. Perimeter barrier coverage: Full [ ]  Partial [ ]  None [ ]
		3. Asset barrier coverage: Full [ ]  Partial [ ]  None [ ]
	1. Access Points (Include all gates, doors, and other access points):

| Access Point Name | Description | Type | Security Measure Details |
| --- | --- | --- | --- |
| Ex. Gate in west perimeter fence | Hinged gate in chain link fence | Gate | Gate is locked with padlock and chains |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Physical locking mechanism
	1. Assets secured by:

| Asset Name | Physical Locking Mechanism |
| --- | --- |
| Ex. Chlorine Storage Cage | Cage is locked with keyed padlock |
|  |  |
|  |  |
|  |  |

* 1. Key and credential inventory
		1. Frequency of inventory: Click or tap here to enter text.
		2. Inventory conducted by: Click or tap here to enter text.
		3. Discrepancies in inventory are reported to:
		Click or tap here to enter text.
		4. Upon compromise/suspected compromise, locks are:
		[ ]  Rekeyed
		[ ]  Replaced
		[ ]  No action
		[ ]  Other (Describe): Click or tap here to enter text.
		5. Upon termination/departure of employees, keys/credentials are collected: Yes [ ]  No [ ]
1. Access control
	1. Personnel identification program: Yes [ ]  No [ ]
		1. Personnel identification conducted via:
		[ ]  Badges
		[ ]  Uniform
		[ ]  Other (Describe): Click or tap here to enter text.
		2. Credential administration conducted by: Click or tap here to enter text.
		3. Badges are required at the facility: Yes [ ]  No [ ]
		4. Visitor access: Yes [ ]  No [ ]
		If yes, describe: Click or tap here to enter text.
	2. Access control system: Yes [ ]  No [ ]
		1. If yes, type of access control system:
		[ ]  Proximity or smart card reader
		[ ]  Token/fob reader
		[ ]  Biometric reader
		[ ]  Personal access code
		[ ]  Common access code
		[ ]  Other (Describe): Click or tap here to enter text.
2. Inspection and screening
	1. Screening at access points: Yes [ ]  No [ ]
		1. Personnel screening: Yes [ ]  No [ ]
		2. Electronic access control: Yes [ ]  No [ ]
	2. Frequency of vehicle inspection: Click or tap here to enter text.
	3. Vehicle restrictions and parking restrictions: Yes [ ]  No [ ]
	If yes, describe: Click or tap here to enter text.
3. Shipping and receiving procedures
	1. Know-your-customer program: Yes [ ]  No [ ]
	2. Product stewardship program: Yes [ ]  No [ ]
	3. Documentation of:
		1. Sales and purchases to or from manufacturers: Yes [ ]  No [ ]
		2. Sales and purchases to or from third parties: Yes [ ]  No [ ]
		3. Confirmation of shipment arrival: Yes [ ]  No [ ]
	4. Type of customer vetting (Describe): Click or tap here to enter text.
	5. Titles of procedures for controlling activities related to purchase and sale:
	Click or tap here to enter text.

Additional Security Measures

If gaps in delay capabilities were identified for any of the chemical assets listed in this section of the security plan, consider what additional security measures might be needed to close the identified gap. In this portion, identify specific security measures that your facility will plan to implement in the future to ensure delay.

Tip: Include a timeline and point of contact responsible to ensure accountability and project completion.

Click or tap here to enter text.

Response

Response within the security plan context primarily refers to the response of appropriately trained personnel—either facility personnel or external first responders—to a threat to or actual theft, release, or sabotage of dangerous chemicals. However, it also includes mitigating the consequences of an incident and the reporting of suspicious behavior or a security incident internally and externally in a timely manner.

Due to the broad scope of this security goal, an appropriate response plan should then involve not only designated facility emergency response personnel, but also all facility personnel (including security personnel), local law enforcement, and other offsite first responders.

Response measures should address the identification of hazards, the corresponding response plans for those hazards, the number and capabilities of the various responders, and the equipping and training of the response personnel. Properly equipped personnel who understand the potential consequences of a security incident and the need for timely, effective actions, coupled with well-rehearsed response plans, reduce the probability of an attack achieving the adversaries’ desired goals.

Additionally, practiced response plans help ensure that onsite responders and local law enforcement, fire, medical, emergency management, mutual aid, and rescue agencies are familiar with the facility and the chemicals stored on site and are not impeded from reaching the location of the security incident.

Directions

* Assess how your facility currently responds to the theft, release, or sabotage of dangerous chemicals.
* When you have identified the current security measures and plans in place, compare them to the security principles laid out in Part 1, Section 5, Response of ChemLock: Secure Your Chemicals ([cisa.gov/chemlock-security-plan](https://www.cisa.gov/chemlock-security-plan)).
* Use this portion of the security plan to ensure each security measure is properly implemented and confirm whether it covers the chemical asset area.
* Identify any gaps in response capabilities and any additional security measures that may be necessary to close those gaps.
* Develop a plan to implement any additional security measures.
* Consider your relationships with local law enforcement and emergency planning committees.

Notes

Click or tap here to enter text.

Response Security Measures

1. Emergency response procedures and crisis management plan
	1. Emergency/security response organization and program: Yes [ ]  No [ ]
		1. Designated individual responsible for response:
		Click or tap here to enter text.
		2. Emergency management team:

| Name | Title | Role in Response |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

* 1. Crisis management plan: Yes [ ]  No [ ]
		1. Title: Click or tap here to enter text.
		2. Issue or revision date: Click or tap here to enter text.
		3. Plan includes (Select all that apply):
		[ ]  Contingency/continuity of operations (COOP)
		[ ]  Emergency response/shutdown/re-entry/evacuation
		[ ]  Media response
		[ ]  Security response plan
		[ ]  Post-incident actions
		[ ]  Other (Describe): Click or tap here to enter text.
	2. Documented response agreements with offsite response services:
	Yes [ ]  No [ ]
	If yes, titles of agreements: Click or tap here to enter text.
	3. Response drills and exercises: Yes [ ]  No [ ]
	If yes, frequency of drills and exercises: Click or tap here to enter text.
1. Outreach Programs
	1. Information sharing/meet-and-greet
		1. Dates for local law enforcement contact: Click or tap here to enter text.
		2. Dates for local fire department contact: Click or tap here to enter text.
		3. Dates for Local Emergency Planning Committee (LEPC) participation:
		Click or tap here to enter text.
		4. Dates for contact with other officials (Specify the official):
		Click or tap here to enter text.
	2. Joint initiatives and exercises (Describe): Click or tap here to enter text.
2. Security plans for elevated threats
	1. Title of policy for elevated threats: Click or tap here to enter text.
	2. Awareness of National Terrorism Advisory System (NTAS) bulletins and alerts: Yes [ ]  No [ ]
	3. Security measures increased during elevated threats: Yes [ ]  No [ ]
	If yes, describe: Click or tap here to enter text.
	4. Imminent threat alert (Describe): Click or tap here to enter text.

Additional Security Measures

If gaps in response capabilities were identified for any of the chemical assets listed in this section of the security plan, consider what additional security measures might be needed to close the identified gap. In this portion, identify specific security measures that your facility will plan to implement in the future to ensure response.

Tip: Include a timeline and point of contact responsible to ensure accountability and project completion.

Click or tap here to enter text.

Cyber

Because cyber systems and the network they operate on are often integrated throughout the operations of chemical facilities, defending against adverse cyber events is essential to the management of the overall risk for a facility. Facilities deter cyber sabotage and minimize the consequences of physical events through the protection of cyber systems. This includes preventing unauthorized access to critical process controls—such as Supervisory Control and Data Acquisition (SCADA) systems, Access Control Systems (ACSs), Distributed Control Systems (DCSs), Process Control Systems (PCSs), Industrial Control Systems (ICSs)—critical business systems, and other sensitive computerized systems. Facilities should consider how best to include comprehensive cybersecurity policies, practices, and personnel to handle adverse cyber events and mitigate their effects.

Directions

* For each cyber asset, describe the location at your site and how it is used.
* Assess how your facility currently provides cybersecurity capabilities and supports the prevention of unauthorized access to cyber systems.
* When you have identified the current security measures, compare them to the security principles laid out in Part 1, Section 6, Cybersecurity of ChemLock: Secure Your Chemicals ([cisa.gov/chemlock-security-plan](https://www.cisa.gov/chemlock-security-plan)).
* Use this portion of the security plan to ensure each security measure is properly implemented and confirm whether it applies to the chemical asset area or system.
* Identify any gaps in cybersecurity capabilities and any additional security measures that may be necessary to close those gaps.
* Develop a plan to implement any additional security measures.
* Consider your facility’s existing cyber systems—to include operational technology (OT) and information technology (IT)—as well as those systems connected to physical security systems, such as IDS or ACS, when conducting this assessment and assigning security measures.

Notes

Click or tap here to enter text.

Cyber Assets

| Cyber System Type | Cyber Asset Name | Location and Description |
| --- | --- | --- |
| Ex. SCADA system | ABC SCADA system for XYZ process | ABC SCADA system is connected to and controls the centrifuge mixing chemicals on machine #1 |
| Ex. Ordering and Inventory Management | 123 Ordering | Located onsite and controls the ordering of all chemicals at the site as well as the management of inventory. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Cybersecurity Measures

1. Cybersecurity policies and procedures
	1. Change management process: IT and OT cultural and technical procedures to safeguard systems (e.g., adding devices, air gaps, etc.): Yes [ ]  No [ ]
	2. Security procedures for employees, system/vendor maintenance, and visitors/contractors using IT and ICS systems: Yes [ ]  No [ ]
	3. Procedures to audit/validate/verify cyber controls: Yes [ ]  No [ ]
	4. Procedures/contract to ensure system security and maintenance from third-party cyber support: Yes [ ]  No [ ]  N/A [ ]
	5. Policies and procedures maintained by: Click or tap here to enter text.
2. Access control and password management
	1. Network accounts and access
		1. List of requested accounts and approved access: Yes [ ]  No [ ]
		2. Unique accounts: List of privileged accounts (e.g., domain administrator, local admin): Yes [ ]  No [ ]
		3. Least privilege: Process for granting only required system/data access: Yes [ ]  No [ ]
		4. Access control lists: Process for managing access for changing roles of employees (e.g., changing positions): Yes [ ]  No [ ]
		5. Access control rules of behavior: Procedures describing IT user responsibilities and expected behavior: Yes [ ]  No [ ]
	2. Password management
		1. Procedures for changing default passwords: Yes [ ]  No [ ]
		2. Procedures for password rules: Yes [ ]  No [ ]
	3. Physical access to cyber systems and information storage
		1. Physical security in place to safeguard equipment from unauthorized access: Yes [ ]  No [ ]
		If yes, describe: Click or tap here to enter text.
	4. External connections
		1. Managing connectivity and ability to transfer data (e.g., external access, wireless connections, etc.): Yes [ ]  No [ ]
		If yes, describe: Click or tap here to enter text.
	5. System boundaries
		1. Policy for all IT technical assets and limiting system access points:
		Yes [ ]  No [ ]
		If yes, title of policy: Click or tap here to enter text.
3. Cybersecurity employee training and process
	1. Cybersecurity awareness training is required for:
	[ ]  All personnel
	[ ]  Security personnel only
	[ ]  Other (Describe): Click or tap here to enter text.
	2. Schedule/record of required cybersecurity training: Yes [ ]  No [ ]
	If yes, maintained by: Click or tap here to enter text.
	3. List of required training, procedures, and policies for new employees:
	Yes [ ]  No [ ]
	If yes, maintained by: Click or tap here to enter text.
	4. Procedures for conducting and documenting training: Yes [ ]  No [ ]
	If yes, maintained by: Click or tap here to enter text.
4. Cybersecurity controls, monitoring, response, and reporting
	1. Intrusion detection or intrusion prevention system: Yes [ ]  No [ ]
	If yes, describe: Click or tap here to enter text.
	2. Regular anti-malware software and other software updates: Yes [ ]  No [ ]
	3. Procedures to manage lifecycle of IT and ICS system components from acquisition to disposal: Yes [ ]  No [ ]
	4. Cybersecurity incident reporting (Select all that apply):
	[ ]  CISA Central (Central@cisa.dhs.gov)
	[ ]  Facility Cybersecurity Officer
	[ ]  Other (Describe): Click or tap here to enter text.
5. Disaster recovery and business continuity
	1. Audits to review compliance with facility’s cybersecurity policies: Yes [ ]  No [ ]
	If yes, frequency of audits: Click or tap here to enter text.
	2. Processes and procedures for (Select all that apply):
	[ ]  Backup and security storage information
	[ ]  Operating the control system environment in manual mode
	[ ]  Backup media
	[ ]  Network diagram
	[ ]  Testing
	[ ]  Other (Describe): Click or tap here to enter text.
	3. Processes and procedures maintained by: Click or tap here to enter text.

Additional Security Measures

If gaps in cybersecurity capabilities were identified for any of the chemical assets listed in this section of the security plan, consider what additional security measures might be needed to close the identified gap. In this portion, identify specific security measures that your facility will plan to implement in the future to ensure cybersecurity.

Tip: Include a timeline and point of contact responsible to ensure accountability and project completion.

Click or tap here to enter text.

Policies, Plans, and Procedures

This section covers recommendations for maintenance of security equipment, training of personnel, employee background checks, incident reporting and investigation, security organization and officials, and recordkeeping.

Directions

* Assess the policies, plans, and procedures currently in place at your facility to manage security measures.
* When you have identified the current policies, plans, and procedures, compare them to the security principles laid out in Part 1, Section 7, Policies, Plans, and Procedures of ChemLock: Secure Your Chemicals ([cisa.gov/chemlock-security-plan](https://www.cisa.gov/chemlock-security-plan)).
* Use this portion of the security plan to ensure each policy, plan, or procedure is properly implemented.
* Identify gaps in current policies, plans, and procedures for which additional policies, plans, or procedures may be necessary to close those gaps.
* Develop a plan to develop and implement any additional policies, plans, and procedures.
* For each item listed below, identify the name of the corresponding policy, plan, and procedure, and any pertinent information regarding its implementation.
* Consider including the plan for each item directly within this plan.

Notes

Click or tap here to enter text.

Policies, Plans, and Procedures to Implement Security Measures

1. Maintenance, inspection, and testing of security equipment program
	1. Maintenance policy: Yes [ ]  No [ ]
		1. Title of policy: Click or tap here to enter text.
		2. Policy includes (Select all that apply):
		[ ]  Procedures to mitigate failure of security systems/equipment
		[ ]  Policy for reporting and correcting deficiencies
		[ ]  Policy for reporting nonroutine outages, failures, and malfunctions
		[ ]  Other (Describe): Click or tap here to enter text.
	2. Testing and inspection policy: Yes [ ]  No [ ]
		1. Title of policy: Click or tap here to enter text.
		2. Policy includes (Select all that apply):
		[ ]  Restricted areas/fence line
		[ ]  Access doors/gates
		[ ]  Vehicle barriers
		[ ]  Lighting
		[ ]  Locking mechanisms
		[ ]  IDS
		[ ]  Cameras
		[ ]  ACS
		[ ]  Other (Describe): Click or tap here to enter text.
2. Security awareness and training program
	1. Site Security Officer training includes (Select all that apply):
	[ ]  Security laws/regulations
	[ ]  Threats
	[ ]  Duties/responsibilities
	[ ]  Drills and exercises
	[ ]  Inspection/screening methods
	[ ]  Other (Describe): Click or tap here to enter text.
	2. Security personnel training includes (Select all that apply):
	[ ]  Security threat/patterns
	[ ]  Communications
	[ ]  Emergency procedures/continency plans
	[ ]  Operation of security equipment/systems
	[ ]  Testing/calibration/maintenance of security systems
	[ ]  Inspection/screening methods
	[ ]  Other (Describe): Click or tap here to enter text.
	3. All employees training includes (Select all that apply):
	[ ]  Recognizing suspicious activity/security incident
	[ ]  Reporting suspicious activity/security incident
	[ ]  Emergency procedures
	[ ]  Security systems/equipment operation
	[ ]  Other (Describe): Click or tap here to enter text.
	4. Training methods (Select all that apply):
	[ ]  Face-to-face
	[ ]  Online
	[ ]  Handouts/bulletin boards
	[ ]  Hands-on activities
	[ ]  Other (Describe): Click or tap here to enter text.
	5. Frequency of tabletop exercises:
	[ ]  Weekly
	[ ]  Monthly
	[ ]  Quarterly
	[ ]  Semi-annually
	[ ]  Annually
	[ ]  Biannually
	[ ]  Other (Describe): Click or tap here to enter text.
	6. Frequency of functional exercises:
	[ ]  Weekly
	[ ]  Monthly
	[ ]  Quarterly
	[ ]  Semi-annually
	[ ]  Annually
	[ ]  Biannually
	[ ]  Other (Describe): Click or tap here to enter text.
	7. Frequency of full-scale exercises:
	[ ]  Weekly
	[ ]  Monthly
	[ ]  Quarterly
	[ ]  Semi-annually
	[ ]  Annually
	[ ]  Biannually
	[ ]  Other (Describe): Click or tap here to enter text.
3. Employee background checks
	1. List of employees with access to chemicals: Yes [ ]  No [ ]
	If yes, maintained by: Click or tap here to enter text.
	2. Employees with access to chemicals require:
		1. Verification of identity: Yes [ ]  No [ ]
		If yes, acceptable documents include: Click or tap here to enter text.
		2. Verification of legal authorization to work (i.e., I-9, eVerify):
		Yes [ ]  No [ ]
		3. Criminal background investigation: Yes [ ]  No [ ]
		4. Other (Describe): Click or tap here to enter text.
	3. Adjudication of background checks completed by:
	Click or tap here to enter text.
		1. Disqualifying issues (Describe): Click or tap here to enter text.
		2. Adjudication completed on a case-by-case basis: Yes [ ]  No [ ]
4. Insider threat
	1. Insider threat policy: Yes [ ]  No [ ]
	If yes, title of insider threat policy: Click or tap here to enter text.
	2. Insider threat program training: Yes [ ]  No [ ]
	3. Procedures for reporting insider threat: Yes [ ]  No [ ]
	If yes, maintained by: Click or tap here to enter text.
5. Visitor escort
	1. Visitor escort policy: Yes [ ]  No [ ]
	If yes, title of visitor escort policy: Click or tap here to enter text.
6. Incident reporting and investigations
	1. Process for incident reporting and investigations: Yes [ ]  No [ ]
	If yes, title of policy for incident reporting and investigations:
	Click or tap here to enter text.
	2. List of reported incidents: Yes [ ]  No [ ]
	If yes, maintained by: Click or tap here to enter text.
	3. CISA Central (Central@cisa.dhs.gov) is included in reporting protocol:
	Yes [ ]  No [ ]
7. Officials, organization, and records
	1. Policy or chart for security organization: Yes [ ]  No [ ]
	2. Policy for Facility Security Officer: Yes [ ]  No [ ]
	3. Policy for retaining security records: Yes [ ]  No [ ]

Additional Security Measures

If gaps in policies, plans, and procedures were identified for any of the chemical assets listed in this section of the security plan, consider what additional policies, plans, and procedures might be needed to close the identified gap. In this portion, identify specific policies, plans, and procedures that your facility will plan to develop and implement in the future.

Tip: Include a timeline and point of contact responsible to ensure accountability and project completion.

Click or tap here to enter text.

[Insert organization branding on the back cover as desired.]