

*Insert Facility/Institute Logo Here*

**STANDARD OPERATING PROCEDURE (SOP) *TEMPLATE***

|  |  |
| --- | --- |
|  | |
| Facility: | |
| SOP Title: *Physical Security SOP* | |
| Document Number: *SOP-012-OP* | Version Number: *01* |
| Process Leader: | Effective Date: *MM-DD-YYYY* |
| Other documents cross-referenced in this SOP (i.e., manuals, SOPs, forms, records):   * Biorisk Management Manual: Chapter V, Biorisk Assessment; Chapter VI, Emergency and Incident Planning, Chapter VII, Personnel Management; Chapter IX, Facility Access Determination; Chapter X, Entry and Exit Procedures; Chapter XI, Facility and Infrastructure; Chapter XIII, Work Practices; Chapter XV, Material Control and Accountability; Chapter XVI, Physical Security Systems; Chapter XVII, Information Control; Chapter XIX, Waste Handling and Disposal; Chapter XX, Transportation and Shipping; Chapter XXI, Emergency and Incident Response, Reporting and Investigation; Chapter XXII, Biorisk Management System Assessment and Improvement) (*4-00-001*) * Biosecurity Program Plan (*6-01-001)* * External Transport and Shipping Security SOP (*SOP-0009-OP)* * Material Control and Accountability SOP (*SOP-010-OP*) * Personnel Reliability SOP (*SOP-011-OP*) * Information Security SOP (*SOP-013-OP*) * Secured Area Access Authorization Record * Secured Area Access Request Form * Key and Code Control Form * Secured Area Access Log | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| Revision Number | Sections Changed | Description of Change | Date | Approved By |
|  |  |  |  |  |

INSTRUCTIONS: The Biorisk Management Manual and supporting Standard Operating Procedure (SOP) templates provide a general overview of common considerations and information that should be addressed within a biorisk management system and program. These templates are not exhaustive and facilities must customize each document to ensure it is locally applicable and relevant. This SOP template provides guidance on the range of specific types of mitigation measures that can illustrate graded and balanced mitigations for physical security. The Biosecurity Program Plan provides specific guidance on how physical security; information security; transportation and shipping; personnel management; and material control and accountability interact with each other (so that you are balanced between these focus areas and within this information security focus area), and what should be considered for full implementation of biosecurity in terms of each focus area. Each focus area should be addressed, as mitigation efforts in only one or a few focus areas are insufficient to provide adequate biosecurity.

* **Black text** can be considered generic text which may be appropriate for inclusion in a facility’s biorisk management manual and SOPs.
* ***Red text*** should be considered guidance or examples and must be reviewed and replaced with facility-specific information.

1. Purpose

The purpose of this document is to establish the procedures for physical security in *[Insert Facility Name]* to ensure graded, layered and balanced physical security system, supported by sound policies and procedures that enable it to be resilient and adaptive.

1. Scope

This document applies to all personnel and visitors within the *[Insert Facility Name]*.

1. Responsibilities

* Top and Senior Management will:
  + aid an organization to develop and enforce a biorisk management program: a set of tools, information and associated actions that are overseen, enforced and continuously improved upon by an organization’s senior management. This will ensure that a biorisk management system is properly implemented and maintained
* The Biorisk Management Committee:
  + is an institutional committee created to act as an independent review group for biorisk management issues; it reports to senior management
  + membership on the biorisk management committee should reflect the different occupational areas of the organization as well as its scientific expertise
* Process Leader ensures that:
  + This SOP is established and implemented effectively to include physical security incident investigations, reporting and corrective actions
  + Authorized users are trained on this procedure and competent prior to reliance on the prescribed security measures
* Facility personnel:
  + Follow the procedures outlined in this SOP
  + Report any problems to the Process Leader
* Scientific *Manager/Director:*
  + Determines the areas, information and items to be secured based on risk assessment and applicable local, national, and international guidelines, standards, and regulations
  + Determines physical security policies and procedures that oversee and ensure access of appropriate individuals to physically secured areas and the prevention of unauthorized access.
  + Determines which personnel are given the authority to grant, enforce, change, temporarily withdraw, or permanently terminate access to physically secured areas
* Security *Manager/Officer*:
  + Provides expertise on effective and proportionate biosecurity measures to the team for risk assessment; may support investigations into incidence of biosecurity; may provide regular security checks
* Biorisk Management Advisor:
  + Provides advice and guidance on biorisk management issues. The role and knowledge of the biorisk management advisor is key to develop, implement, maintain and continually improve a biosafety and biosecurity program based on a management system
* Members of the Workforce:
  + All members of the workforce are responsible for the proper implementation of physical security measures

1. Preparation *(Anything that needs to be in place prior to commencing the procedure)*
   1. Materials

* Valuable and/or sensitive materials, equipment, information and information systems *(as defined by the Scientific* *Manager/Director such as collections and reference strains of especially dangerous pathogens, sensitive information storage cabinets or computers, expensive assets, dual-use equipment, etc.)*
* Relevant architectural plans
* Topographical and satellite maps of the surrounding area
  1. Equipment
* *Computers (if using electronic database)*
* *Access control hardware (e.g., locks, lockable doors, lockable windows, fencing)*
* *Access control software (e.g., access keypads, RFID)*
* *Personnel identification linked to permission to access the facility*
* *Visitor Identification*
* *Surveillance capability (e.g., reception desk, video recording)*
  1. Records and Forms *(to be retained for a period of time [e.g., five years, three years after an employee leaves the facility] as defined by the Scientific Manager/Director)*
* Comprehensive risk assessment
* Personnel and Visitor Access Management System *(i.e., paper-based/notebook, electronic/spreadsheet/database)* and associated form(s) to grant individuals access to the facility and/or subparts of the facility (refer to Attachment B, Facility Access Authorization Log) and associated form(s) for personnel vetting, granting/changing/withdrawing/termination of access
* Secured Area Access Log
* Facility Access Request Form
* Key and Code Control Form
* Incident Response Form and Log
* *Memoranda of Understanding with local Emergency Response*
* *Third party records (e.g., contracts, agreements, personnel backgrounds, physical security assessments and features of vendors, suppliers, etc.)*

1. Procedure *(refer to Attachment A, Physical Security SOP Template Flow Chart)*
   1. Identify Assets Requiring Physical Security
      1. *Describe steps to determine the areas, information and items that need to be secured using questions and comments from flow chart step 1*
   2. Describe Current Security Features
      1. *Identify steps to describe existing security features including a description of their adequacy, whether they provide low-, medium- or high- security using questions and comments from flow chart step 2*
   3. Identify a Graded Physical Security Scheme
      1. *Describe steps to determine the degree of physical security needed around the assets identified in flow chart step 1, in a manner that gives the most valuable/sensitive assets the highest degree of security, using questions and comments from flow chart step 3*
   4. Layer the Physical Security Scheme
      1. *Describe steps to determine the layers of physical security, at the appropriate grade, that can and should be secured around those assets identified in flow chart step 1, including by relocating assets, using questions and comments from flow chart step 4*
   5. Balance the Physical Security Scheme
      1. *Describe steps to determine the physical security measures that would result in balanced physical security scheme using questions and comments from flow chart step 5*
   6. Design
      1. *Describe steps to design/redesign the facility, if necessary, to make the most of existing security features, incorporate desired new security features, and accommodate future security features and upgrades using comments and questions from flow chart step 6 (e.g., relocating items to areas which are easier to provide security for, incorporating security features in designs for remodels or future installations, incorporate needed features and anticipated future features or upgrades)*
   7. Establish Security Policy
      1. *Describe steps to determine how physical security is implemented and enforced using comments and questions from flow chart step 7 (e.g., define who is allowed access to secure areas; who has the authority to deny access; how access is granted, changed and revoked; requirements for personnel to report unusual events, implement protocols correctly, report lost/stolen items immediately, and never share security details with unauthorized persons)*
   8. Establish Security Personnel
      1. *Describe steps to determine who is responsible for enforcing security policy using comments and questions from flow chart step 8 (e.g., facility security personnel, third party security firms)*
   9. Establish Security Procedures
      1. *Based on the existing and planned security features, describe steps to provide and limit physical access to secured spaces, materials, equipment, information and information systems using comments and questions from flow chart step 9 (e.g., providing access methods to appropriate staff, establishing the procedures they use to access the spaces, procedures to be followed for visitors and third parties, procedures to be followed to withdraw access from individuals)*
   10. Establish Which Individuals Will Have Access
       1. *Describe steps to determine who can access which physically secured areas, materials, equipment, information and information systems, and when, using comments and questions from flow chart step 10*
   11. Install/Improve
       1. *Describe steps to install, establish and/or improve security measures to meet physical security needs, as defined in flow-chart steps 1-6, using questions and comments from flow chart step 11 (e.g., perimeters and boundaries, access control, video recording, sensors, alarms, guard stations, communications)*
   12. Provide
       1. *Describe steps to provide approved individuals with the knowledge, items and techniques they require to access the secured spaces, materials, equipment, information and information systems using comments and questions from flow chart step 12 (e.g., training, keys, codes)*
   13. Verify
       1. *Describe steps to verify that approved individuals are able to access the secured items they require, and that unauthorized individuals are unable to access them, using comments and questions from flow chart step 13 (e.g., testing with security staff and employees, testing by an appropriate third party)*
   14. Reinforce
       1. *Describe steps to reinforce adherence to physical security policy using comments and questions from flow chart step 14 (e.g., distributing a code of conduct, reminder messages, re-enforcing postings)*
   15. Improve resiliency of feature
       1. *Describe steps to install or establish methods which ensure physical security features are less likely to fail when subjected to human, environmental or utility interference using comments and questions from flow chart step 15 (e.g., generator back-up; mechanical fail-safes; resistant to elements, electrical, and radiofrequency interference; resistance to tampering)*
   16. Maintain security features
       1. *Describe steps to complete scheduled performance testing and preventative maintenance using comments and questions from flow chart step 16*
   17. Monitor
       1. *Describe steps to determine when and how physically secured areas, materials, equipment, information and information systems are monitored using questions and comments from flow chart step 17 (e.g., continuous video surveillance, motion-activated video recording, unannounced inspections)*
   18. Investigate
       1. *Describe steps to further investigate a physical security incident to include real-time assessments and post-incident investigations using questions and comments from flow chart step 18*
   19. Report
       1. *Describe steps and time constraints for reporting physical security incident investigative findings using questions and comments from flow chart step 19 (e.g., logs of access, records of incident investigation findings)*
   20. Review Access
       1. *Describe steps to determine when and how personnel are re-evaluated for access need and appropriateness using questions and comments from flow chart step 20*
   21. Change Access
       1. *Describe steps to upgrade, downgrade, temporarily withdraw or permanently terminate the physical access that a specific individual has using questions and comments from flow chart step 21 (e.g., upon failure to complete physical security training, upon failure to adhere to physical security procedures or policies, lack of future need for access, need for increased future access, discontinuation of employment)*
   22. System Validation and Reconciliation
       1. *Describe steps to reconcile and validate the physical security of the facility using questions and comments from flow chart step 22* *(e.g.,* *scheduled performance testing, re-validations brought on by change, required reconciliations suggested by incidents)*
2. References
   1. World Health Organisation (WHO), Laboratory Biosafety Manual, 4th Edition, <https://www.who.int/publications/i/item/9789240011311>
   2. World Health Organisation (WHO), Biorisk Management: Laboratory Biosecurity Guidance, September 2006, <http://www.who.int/csr/resources/publications/biosafety/WHO_CDS_EPR_2006_6.pdf>
   3. Salerno, RM and Gaudioso, J. Laboratory Biosecurity Handbook, CRC Press, Boca Raton, FL, 2007
   4. International Organization for Standardization. (2019). *Biorisk management for laboratories and other related organisations* (ISO Standard No. 35001:2019). <https://www.iso.org/standard/71293.html>
   5. Centers for Disease Control and Prevention (CDC)/National Institutes of Health (NIH), Biosafety in Microbiological and Biomedical Laboratories (BMBL), 6th Edition,

<https://www.cdc.gov/labs/BMBL.html>

1. Attachments
   1. Physical Security SOP Template Flow Chart
   2. Secured Area Access Authorization Record
   3. Secured Area Access Request Form
   4. Key and Code Control Form
   5. Secured Area Access Log