Attachment A, Physical Security

* *What areas should be considered for physical security measures based on the sensitive or valuable nature of the spaces, materials, equipment, information and information systems within (e.g., potentially pandemic pathogens, dual-use equipment, financially valuable collections, classified information storage cabinets or computers)*
* *Are there regulatory requirements or guidelines to be met?*
* *Refer to Biorisk Management (BRM) 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 Equipment; 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) and the Biosecurity Program Plan (6-01-001)*

SOP Template Flow Chart

* *Describe the type of security measures that are present (e.g., lock with a key, keypad requiring a standard code, radio-frequency identification reader, security guard)*
* *Describe the hardness of that security measure against physical force (e.g., wood door with wood frame, solid composite door with composite frame and multiple locks, steel reinforced door with hardened steel frame and steel bolt closures)*
* *Describe all features of the facility and grounds that impact physical security, and how they increase or decrease the likelihood of unauthorized access or break-in (e.g., topography, foliage, perimeters and boundaries, sensors, communications)*

**1**

Identify Assets Requiring Physical Security

**2**

Describe Current Security Features

* *Describe steps to determine how physical security is implemented (e.g., define who is accountable for arranging and installing the security and design features identified above, define who is allowed access to secure areas and who has the authority to deny access; how access is granted, changed and revoked)*
* *Describe steps to determine what is expected of personnel (e.g., requirements for personnel to report unusual events, implement protocols correctly, report lost/stolen items immediately, never share security details with unauthorized persons)*
* *Describe steps to determine how physical security expectations are enforced (e.g., what violations of which expectations are associated with which disciplinary actions, who has the authority to enact those disciplinary actions)*
* *Identify which individuals oversee granting, changing or revoking personnel access permissions*
* *Identify which personnel are responsible for verifying that physical security measures function properly*
* *Identify which personnel are responsible for monitoring and enforcing the real-time access of physically secured areas (e.g., at the security desk, in the video monitoring room)*
* *Identify which personnel respond to an incident and have the authority to detain unauthorized persons*
* *Which personnel have the authority to bring in local law enforcement to help respond to an overwhelming incident?*
* *Describe how you will create equal mitigation layers for an adversary to face, regardless of the path chosen to the targeted asset*
* *Describe how you will ensure an equal quality of materials at the perimeter of each layer of security (e.g., are the door and door frame as sturdy as the lock? are there windows that are easily broken?)*
* *Describe how you will ensure there a distribution of security measures at different layers such that the skills required to overcome them are sufficiently specialized and varied (e.g., to overcome one requires ability to copy a key, but to overcome the next requires a coded badge and a unique password)?*
* *When designing new facilities, describe how the security measures desired plus the ability to upgrade and add future security measures factored into the design*
* *Describe how re-doing the layout of the rooms or the changing the location of certain activities within the building accomplishes some of your physical security goals*
* *Describe if and where minor construction is needed to install new walls or barriers*
* *Describe if and how the surrounding landscape should be changed improve the security posture of the facility (e.g., to create better visibility, prevent hostile actors from driving onto the property or into the building)*
* *Confirm that there are layers of security that advance in severity to a level appropriate to the assets therein (e.g. a low-security protected area surrounds the entirety of the medium security area, the medium security area completely surrounds the high security area)*
* *Describe where items can be relocated to achieve this layering effect*
* *Describe new security measures or design features required to achieve the needed layering*
* *Using information gained from the risk assessment, what level of physical security is needed for each asset, matched to the relative sensitivity or value of that asset (e.g., potentially pandemic pathogens requiring a high level of security while outdoor walking paths require a lower level of security)?*
* *Based on the existing and planned security features, describe steps to provide physical access to secured spaces, materials, equipment, information and information systems to those who are authorized (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)*
* *Based on the existing and planned security features, describe steps to limit physical access to secured spaces, materials, equipment, information and information systems (e.g., procedures to be followed to turn away individuals who are not authorized to access an area; procedures to be followed to remove keys, badges, codes and any other means of accessing a secured area from individuals who lose authorization that area)*

**9**

Establish Security Procedures

**8**

Establish Security Personnel

**7**

Establish Security Policy

**6**

Design

**5**

Balance the Physical Security Scheme

**4**

Layer the Physical Security Scheme

**3**

Identify a Graded Physical Security Scheme

Security Procedures

Security Policy

* *Describe steps to inform responsible personnel of the findings of physical security incident investigations*
* *Delineate time constraints for submission of the report*
* *Describe how the system is validated (e.g., auditing and access permission reconciliation)*
* *Describe when the system is validated (e.g., scheduled performance testing, re-validations brought on by change, required reconciliations suggested by incidents)*
* *Identify who is notified of discrepancies*
* *Describe how discrepancies are resolved*
* *Describe the process for investigating/evaluating lessons learned/ implementing corrective actions. Track status in Incident Response Form and Log*
* *Refer to BRM Manual: Chapter XXI, Emergency and Incident Response, Reporting and Investigation; Chapter XXII, Biorisk Management System Assessment and Improvement*
* *Identify who is authorized to review the access permissions for employees*
* *Identify when access permission for employees is reviewed (e.g., regularly scheduled reviews, upon reports of unusual behavior or circumstances, upon the report of negative findings on a member of staff after an incident)*
* *Describe steps taken to review the access needs, and appropriateness that a specific person has, to physically secured areas*
* *Describe steps to record the completion and outcome of an access review*
* *Describe process to report the outcomes of an access review to responsible parties, particularly if a change in access is required*
* *Identify who is authorized to change the access permissions for employees*
* *Describe the steps to determine whether access permissions should be changed (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)*
* *Describe steps to upgrade the physical access that a specific individual has*
* *Describe the steps to downgrade the physical access that a specific individual has*
* *Describe the steps to temporarily withdraw the physical access that a specific individual has*
* *Describe the steps to permanently terminate the physical access of a specific individual*
* *Describe steps to digitally monitor and record access to secured spaces (e.g., digital logging of keycard or keycode access times and individuals’ logons or access code use for equipment inside the space, motion sensors)*
* *Describe steps to visually monitor and record access to secured spaces (e.g., guards with access logs, video monitoring)?*
* *Describe who investigates a security incident*
* *Describe when security incidents are investigated (e.g., real-time assessments, post-incident investigations)*
* *Describe steps to investigate an incident*
* *Describe steps to record findings in an investigation*
* *Describe steps to perform and document scheduled performance testing of security measures*
* *Describe steps to perform and document preventative maintenance of security measures*
* *Describe steps to regularly check for updates and upgrades available for security measures*
* *Describe steps to determine whether physical security measures function properly (e.g., doors latching when closed, locks properly engaging, gates closing)*
* *Describe steps to determine if physical security measures allow access to approved personnel (e.g., keys work in locks, codes work on keypads)*
* *Describe steps to determine if physical security measures prevent access to unauthorized individuals (e.g., locks easy to pick, door jambs not sturdy enough to prevent break-ins, codes too easy to duplicate)*
* *Describe the steps to establish security measures to meet physical security needs (e.g., closing doors and engaging pre-existing locks, posting guards at key locations, moving sensitive or valuable items to more secure locations)*
* *Describe steps to install security measures to meet physical security needs (e.g., installing access keypads and/or card-readers, cameras, walls, doors and/or reinforced glass)*
* *Describe the steps to improve security measures to meet physical security needs (e.g., upgrades to perimeters and boundaries, adding permanent non-overlapping recording to video systems, providing advanced response training to security personnel, establishing contact numbers and guidance)*
* *Based upon Security Policy, describe steps to determine which individuals in the facility require access to which secured areas*
* *Describe steps to maintain a current list of individuals requiring access to particular areas, connected to the methods by which they are accessing those areas*
* *Describe steps to remind personnel of the expectations placed on them with regard to physical security measures*
* *Describe steps to reward individuals who adhere, without incident, to these expectations*
* *Describe steps to make personnel aware of physical security incidents that have occurred and corrective actions that were taken*
* *Describe steps to provide approved individuals with knowledge on how to gain entry (e.g., formal training, mentorship with an experienced individual, private sessions with security personnel)*
* *Describe steps to provide approved individuals with the items they require to gain entry (e.g., checking out keys, randomly generating unique access codes and assigning them to the individual, programming chips on badges)*
* *Describe steps to provide approved individuals with the techniques they require to gain entry (e.g., training, keys, codes)*

Laboratory Access Request Form

Personnel and Visitor Access Management System

* *Describe steps to improve resiliency of physical security measures (e.g., connecting electrical elements of security features to backup generators, ensuring that the default position of door locks is the locked position)*
* *Describe steps to improve resiliency of physical security personnel (e.g., cross-training of personnel on different security roles; sufficient relief personnel so that breaks, meals and rest cycles can be accommodated even during emergency situations; health and exercise accommodations)*

**21**

Change Access

**22**

System Validation and Reconciliation

**19**

Report

**18**

Investigate

Incident Response Log

Incident Response Form

**14**

Reinforce

**12**

Provide

Key and Code Control Form

**13**

Verify

**15**

Improve Resiliency

**16**

Maintain Security Features

Secured Area Access Log

**20**

Review Access

**17**

Monitor

**11**

Install/Improve

**10**

Establish Which Individuals Will Have Access