

*Insert Facility/Institute Logo Here*

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

|  |
| --- |
|  |
| Facility: |
| SOP Title: *Information Security SOP* |
| Document Number: *SOP-013-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 VII, Personnel Management; Chapter IX, Facility Access Determination; Chapter XVI, Physical Security Systems; Chapter XVII, Information Control; Chapter XIX, Waste Handling and Disposal; Chapter XXI, Emergency and Incident Response, Reporting and Investigation; Chapter XXII, Biorisk Management System Assessment and Improvement) (*4-00-001*)
* Biosecurity Program Plan (6*-00-001)*
* Transport and Shipping Security SOP (*SOP-009-OP*)
* Material Control and Accountability SOP (*SOP-010-OP*)
* Personnel Reliability SOP (*SOP-011-OP*)
* Physical Security SOP (*SOP-012-OP)*
* Sensitive Information Access Authorization Log
* *Record of Sensitive Information Access*
 |

|  |
| --- |
|  |
| 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 information 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 information security in *[Insert Facility Name]*’s to ensure proper handling of sensitive information and information systems during generation, receipt, storage, access, transfer and disposal.

1. Scope

This document applies to all personnel and visitors within *[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 incident investigations, reporting and corrective actions
	+ Authorized users are trained on this procedure and competent prior to independent work involving sensitive information and/or information systems
* Facility personnel:
	+ Follow the procedures outlined in this SOP
	+ Report any problems to the Process Leader
* Scientific *Manager/Director:*
	+ Defines sensitive information and information systems to be secured based on risk assessment and applicable local, national, and international guidelines, standards, and regulations
	+ Determines information security processes that oversee and ensure secure generation, receipt, storage, use, transfer and disposal of sensitive information and information systems
	+ Determines which personnel are authorized for access to sensitive information and information systems
* Security Manager/Officer:
	+ *Provides expertise on effective and proportionate facility biosecurity measures to the team for risk assessment; may support investigations into biosecurity incidents; may provide regular security checks*
* Biosafety Officer/Biorisk Management Advisor:
	+ *Provides advice and guidance on biorisk management issues. The role and knowledge of the biorisk 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 security measures
1. Preparation *(Anything that needs to be in place prior to commencing the procedure)*
	1. Materials
* Information of a potentially sensitive nature *(as defined by the Scientific* *Manager/Director such as genomic information from potentially pandemic pathogens, protocols and procedures which could be stolen for nefarious purposes, security features and weaknesses of your facility, personal details of employees, diagnostic results tied to particular patients, protected government or commercial information, etc.)*
* Written records of potentially sensitive information *(such as laboratory notebooks, patient sample books, diagnostic laboratory records, etc.)*
* Information systems containing potentially sensitive information
* Classification guide
	1. Equipment
* *Secured Computer(s) (if using electronic information) (access-controlled, password protected, two-factor authentication, encryption, etc.)*
* *Secure communications (encryption, dedicated land-lines, etc.)*
* *Personnel identification linked to permission to access sensitive information*
* *Locking cabinets*
* *Secure rooms*
* *Redaction methods (e.g., indelible markers indistinguishable from inks used, tear-lines)*
* *Destruction methods (e.g., shredders, incinerators)*
	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)*
* Sensitive Information Access Management System *(i.e., paper-based/notebook, electronic/spreadsheet/database)* and associated form(s) to grant individuals access to sensitive information and information systems (refer to Attachment B, Sensitive Information Access Authorization Log)
* Sensitive Information Access Record
* Record of sensitive information transfer *(e.g., hand-carry form, chain-of-custody document)*
* Discrete coverings for hard-copy documents *(e.g., cover sheets, envelopes, fax cover sheets)*
1. Procedure *(refer to Attachment A, Information Security SOP Template Flow Chart)*
	1. Identify Sensitive Information and Information Systems
		1. *Describe steps to determine the items of information and information systems that need to be secured using questions and comments from flow chart step 1*
	2. Identify Classification Scheme
		1. *Describe steps to determine the classification system and level of information to be included in the classification markings using questions and comments from flow chart step 2*
	3. Marking
		1. *Describe steps to determine when and how existing information and information systems are marked as sensitive using questions and comments from flow chart step 3*
	4. Protection
		1. *Describe measures taken to prevent unauthorized access to sensitive information using questions and comments from flow chart step 4*
	5. Authorization
		1. *Describe when and how a person is granted access to sensitive information and information systems using questions and comments from flow chart step 5*
	6. Access
		1. *Describe steps to determine when and how accessing of sensitive information and information systems is recorded using questions and comments from flow chart step 6*
	7. Generation
		1. *Describe steps to determine when and how information and information systems are marked as sensitive when being created using questions and comments from flow chart step 7*
	8. Receipt
		1. *Describe steps to determine when and how information and information systems with existing markings are received using questions and comments from flow chart step 8*
	9. Transfer
		1. *Describe steps to determine when and how sensitive information and information system transfers are conducted using questions and comments from flow chart step 9*
	10. Storage
		1. *Describe steps to determine where and how to store sensitive information and information systems using questions and comments from flow chart step 10*
	11. Redaction
		1. *Describe steps to determine when and how sensitive information and information systems are redacted using questions and comments from flow chart step 11*
	12. Disposal
		1. *Describe steps to determine when and how sensitive information and information systems are disposed of using questions and comments from flow chart step 12*
	13. System Validation and Reconciliation
		1. *Describe steps to determine when and how the security of sensitive information and information systems is validated to include the incident investigation processes using questions and comments from flow chart step 13*
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. Information Security SOP Template Flow Chart
	2. Sensitive Information Access Authorization Log