



# BIOSAFETY AND BIOSECURITY MANUAL MOBILE BSL-2 LABORATORIES PAKISTAN



**Disclaimer:**

This publication was prepared by the USAID funded, Global Health Supply Chain Program – Procurement and Supply Management (GHSC-PSM) project, managed by Chemonics International Inc. The authors' views expressed in this publication do not necessarily reflect the views of the U.S. Agency for International Development or the United States Government.

Version	Funded by	Approved by	Date of implementation	Applicability
Final	USAID/ Pakistan	National Institute of Health/ MoNHSR&C	July 06, 2022	This is a living document



# Contents

Foreword.....	ix
Acknowledgement.....	xi
Acronyms.....	xiii
Definitions and Terminologies.....	xv
Section I: Introduction.....	I
Profile	I
Purpose	I
Scope	I
Responsibilities	I
Section II: Protocols for Operations, Security, and Response Plan of Mobile Biosafety Level 2 Laboratory .....	3
Defining the RISK	3
Response Management	3
Incident Management and Reporting	5
Accidents	5
Incident Management	10
Section III: Mobile BSL-2 Laboratory .....	11
Salient Features of Mobile BSL-2 Laboratory	11
Security	11
Preventative Maintenance	12
Section IV: Biological Risk Assessment.....	13
Hazard Identification	13
Risk Assessment	13
Risk Characterization	13
Risk Evaluation	13
Risk Reduction	14
Risk Communication	14
Section V: Administrative Control .....	15
Standard Operating Procedures	15
Occupational Health/Medical Surveillance	15
Training	15
Mechanisms for Continuous Improvement	16
Section VI: Work Practices .....	17
Good Laboratory Practices	17
Laboratory Aerosols	18
Section VII: Safety Equipment Primary and Secondary Containment.....	21
Primary Containment	21
Secondary Containment	23

Section VIII: Biological Safety Cabinets.....	25
Classification	25
Biological Safety Cabinets	25
Section IX: Laboratory Waste Management.....	29
Definition:	29
Types of Biological Waste	29
Processes of Waste Management	30
Reuse	34
Recycling	34
Section X: Transport of Infectious/Biological Materials .....	35
Definitions	35
Category A (Infectious Substances)	35
Category B (Biological Substances)	35
Exempt Substances	35
Category A Packaging	36
Category B Packaging	37
Section XI: Biological Emergency Response Procedures and Incident Reporting.....	39
Needlestick or Cut with Contaminated Sharp Item	39
Emergency Evacuation	40
Spill Management	41
Section XII: Decontamination and Disinfection of Laboratory .....	43
Cleaning	43
Disinfection	43
Sterilization	43
Decontamination	43
Section XIII: Biosecurity .....	45
Risk Assessment	45
Physical Protection	46
Personnel Security	46
Inventory Control	46
Information Security	46
Transport Security	46
Emerging Biotechnology	47
Dual-Use Research of Concern	47
References .....	49
Annexes .....	51
Annex 1: Security Management Plan	53
Annex 2: Incident Management Plan	83
Annex 3: Incident Reporting Form	100

Annex 4: Serious Incident Reporting template	105
Annex 5: Event Management	107
Annex 6: Layout plan of the mobile BSL-2 laboratory	113
Annex 7: SOPs for Avoiding Occupational Hazards	115
Annex 8: Rapid Inactivation Protocols	117
Annex 9: Facility Security Plan	119
Annex 10: Risk Assessment Tool	139
Annex 11: Field Certification Protocols for Biosafety Cabinets NSF1/ANSI/49 Standard	143
Annex 12: SOPS for Autoclave	145
Annex 13: Fire Evacuation SOPs	147
Annex 14: SOPs for Laundry	149
Annex 15: Rapid Inactivation Protocols	151
Annex 16: Technical Working Group for Mobile BSL-2 labs	153
KEY CONTRIBUTORS.....	155

**Tables:**

Table 1: Incident Management Committee .....	4
Table 2: List of drivers and contact details (temporary for two months) .....	5
Table 3: List of biomedical engineers and contact details.....	12
Table 4: Classification of Class II Biosafety Cabinets .....	25
Table 5: List best practices for collecting waste from different laboratory sections or departments.....	33
Table 6: Spill kit requirements.....	41

**Figures:**

Figure 1: Islamabad Map with response areas.....	6
Figure 2: Map of Lahore, Punjab with response areas .....	7
Figure 3: Map of Karachi, Sindh with response areas .....	8
Figure 4: Map of Peshawar, Khyber Pakhtunkhwa with response areas .....	9
Figure 5: Risk Assessment Strategy .....	13
Figure 6: Triangle of hierarchy.....	14
Figure 7: Assessment Mitigation Performance Model.....	16
Figure 8: Sequence for donning and doffing of PPE .....	22
Figure 9: Class I Biological Safety Cabinet .....	25
Figure 10: Class II Biological Safety Cabinets .....	26
Figure 11: Class II, Type B2 .....	26
Figure 12: Operational diagram of Biosafety Cabinet.....	27
Figure 13: HEPA filters .....	28
Figure 14: An example of a label for infectious waste .....	31
Figure 15: International hazard symbols.....	31
Figure 16: Example of a triple packaging system for the packaging and labelling of Category A infectious substance (Source: IATA, Montreal, Canada .....	36
Figure 17: Standard triple packet system as per WHO classification for packaging and labelling Category B (Source: IATA, Montreal, Canada.....	37
Figure 18: Needle stick Inquiry.....	39
Figure 19: Yellow Evacuation .....	40

Figure 20: Descending order of relative resistance to disinfectant chemicals .....44  
Figure 21: Elements of Biosecurity .....46



## Foreword

This document will serve as the Biosafety and Biosecurity Manual for Pakistan Mobile Biosafety Level 2 (BSL-2) Laboratories. These laboratories will strengthen Pakistan's diagnostics facilities to manage the current COVID-19 pandemic and emerging public health threats. All essential aspects of biosafety and biosecurity are the primary responsibility of all individuals involved in Mobile BSL-2 laboratories' operations. This obligation includes not only ensuring a safe working environment for coworkers, but also extending safety concerns to individuals working in a mobile context, while caring for communities and the environment. Job performance necessitates not just knowledge and competence, but also an ongoing understanding of the significance of safety, health, and the environment.

This manual has been developed to understand various issues of biosafety and biosecurity when working in mobile laboratory settings under the general supervision of Pakistan Technical Working Group for Mobile BSL-2 Labs<sup>1</sup> and Pakistan Biological Safety Association (PBSA).

The content of this manual must be read, understood, and followed by every member of the mobile team and other related personnel.

Failure to follow these guidelines may result in injury to mobile laboratory personnel, staff members, and patients, and may cause damage to the mobile laboratory's equipment and operations.

---

<sup>1</sup> National Institute of Health, Ministry of National Health Services, Regulations and Coordination - Notification No. F.1-5/2022/PHLD-Admin dated 16<sup>th</sup> May 2022 (Annex 16)



# Acknowledgement

Epidemics and outbreaks are always urgent and require a rapid, safe, and flexible response, with well-functioning laboratory networks, to manage these public health emergencies. The COVID19 pandemic and high mortality and morbidity from vaccines preventable infectious diseases in the country, has led to special emphasis on early detection and containment of viral and other pathogens. The growing number of public health events are leaving catastrophic socio-economic impact on developing economies of the world.

In these testing times, USAID is supporting Pakistan to respond to COVID19 emergency and generating rapid response to epidemics. The provision of Bio Safety Level 2 mobile laboratories will strengthen the indigenous public health laboratory network. These mobile laboratories will enhance the public sector capacity to rapidly deploy a sophisticated biosafety lab infrastructure. It would offer strategic advantages to respond quickly and effectively at entry/exit points, hard to reach remote areas during an emergency outbreak or epidemic.

We proudly put forward the completed version of the Biosafety and Biosecurity Manual. The manual would serve as a guiding document for the designated laboratory staff to ensure safe laboratory operations as per international best practices<sup>2</sup>.

The Ministry of National Health Services, Regulations and Coordination (M/o NHR&C) under the leadership of Secretary is committed to improve the public health delivery system. I am thankful to the NIH laboratory division team, Dr. Salman Ahmed, Dr. Fahim Tahir and Mr. Firdous Khan for their technical contributions in the development of this document.

We acknowledge the invaluable leadership of Dr. Enilda Martin, and Mr. Xerses Sidhwa, Directors, Health Office; and Mr. Khalid Mahmood, Project Management Specialist, USAID Pakistan.

We owe special thanks to Dr. Muhammad Tariq, the Country Director, USAID Global Health Supply Chain Program – Procurement and Supply Management (GHSC-PSM) project, Mr. Wayne Lifshitz, Asia Sr. Director, and their teams in Islamabad and Washington for their devoted efforts and support provided in the formulation of this manual.

In the end, this would have not been possible without the technical expertise of Prof. Dr. Shams-ul-Arfin Qasmi and Prof. Dr. Muhammad Tahir Khadim.



**Prof. Dr. Aamer Ikram**  
Executive Director  
National Institute of Health, Islamabad

---

<sup>2</sup> This living manual is developed by certified biosafety experts of the PBSA, IFBA and American Biological Safety Association. The NIH plans accreditation of this document by the international and national bodies including PNAC



# Acronyms

BMBL	Biosafety in Microbiological & Biomedical Laboratories
BRD	Business Risk Department
BSC	Biosafety Cabinet
BSL	Biosafety Level
BSL-1	Biosafety Level 1
BSL-2	Biosafety Level 2
CCTV	Closed-Circuit Television
CDC	Centers for Disease Control & Prevention
CEN	European Committee for Normalization
CWA	CEN Workshop Agreement
FSM	Facility Security Manager
GB	Gilgit Baltistan
GoP	Government of Pakistan
HEPA	High-Efficiency Particulate Air
HVAC	Heating, Ventilation, and Air Conditioning
IBC	Institutional Biosafety Committee
ICT	Islamabad Capital Territory
IFBA	International Federation of Biosafety Associations
IMT	Incident Management Team
KP	Khyber Pakhtunkhwa
LAI	Laboratory-Acquired Infection
LEA	Law Enforcement Agency
MBL	Mobile Biosafety Laboratory
MC&A	Material Control and Accountability
MONHSRC	Ministry of National Health Services, Regulations and Coordination
MSDS	Material Safety Data Sheets
NIH	National Institute of Health Pakistan
OSRO	Operations, Security and Response Plan Officer
PBSA	Pakistan Biological Safety Association
PNAC	Pakistan National Accreditation Council
PSDS	Patient Safety Data Sheets
RCLS	Responsible Conduct of Life Sciences
SC	Safety Coordinator
SMP	Security Management Plan
SOP	Standard Operating Procedure
SSFP	Security Safety and Focal Person
USAID	United States Agency for International Development
WHO	World Health Organization



# Definitions and Terminologies

Accident	An unplanned event that results in an injury, illness, or damage to property or the environment involving employees, volunteers, contractors, cooperators, emergency personnel, visitors, or the public.
Biohazard	Potential source of harm caused by biological agents or toxins.
Biohazard Incident/Accident	<p>An incident may include exposure of staff or the public to an infectious, potentially infectious, or zoonotic agent; environmental release of a biohazard; escape of infected animals or vectors; spill of a biohazard outside of a primary containment device; loss or theft of biohazardous agents and other loss of containment; or equipment failure in conjunction with a biohazard (e.g., centrifuge accident) that may lead to a release of a hazardous agent within the laboratory environment or outside the laboratory environment.</p> <p>NOTE: A spill occurring inside a functioning biological safety cabinet or similar primary containment device, although undesirable, does not ordinarily constitute a reportable spill/biological incident, if decontamination/inactivation and cleanup activities take place within the primary containment device. Any procedure or protocol that seems to routinely produce conditions that result in gross contamination of the biosafety cabinet should be reported to the laboratory director/research leader so that the procedure can be evaluated and modified.</p>
Bio Risk	Combination of the likelihood of occurrence of harm and the severity of that harm by a biological agent or toxin.
Bio Risk Assessment	Analytical process of assessing the risk arising from a biohazard.
Bio Risk Management System	Part of an organization's management system identified to develop and implement bio risk policy and manage its bio risks.
Biosafety	The containment principles, technologies, and work practices that are implemented to prevent the unintentional exposure to biological agents and toxins or their accidental release.
Biosecurity	The protection, control, and accountability for biological agents and toxins in the laboratories to prevent their loss, theft, misuse, diversion of, unauthorized access or intentional unauthorized release.
Calibration	Correlation of the performance of equipment (e.g., readings of an instrument) to a standard.
Certification	Systematic, documented process to ensure systems perform in accordance with available certification standards or applicable validation guidance.

Decontamination	A process (physical, chemical, or combination) that reduces the level of microbial contamination so that it can be reasonably assumed to be free of risk of infection transmission.
Disinfection	A process to reduce the number of microorganisms, but not usually of bacterial spores without necessarily killing or removing all organisms.
Good Microbiological Techniques	Methods used to eliminate or minimize exposure to biological agents through aerosols, splashes, and accidental inoculation.
Hazard	Source, situation, or act with a potential for causing harm.
Incident	An occurrence (event), natural or human-caused, that happens within the work environment involving biological-associated hazards, including toxins. Incidents can include, but are not limited to, unsafe occurrences and hazardous situations. These could include preventable and non-preventable occurrences, occurrences involving individuals/personnel, or situational events not involving individuals/personnel; and may or may not be accidental.
Personal Protective Equipment	Material, including clothing, gowns, gloves, respirators, and safety glasses used to maximize the risk of exposure to or contamination of a person by chemical or biological hazard.
Mobile Laboratory	That is either fully housed within or transported by a vehicle, such as a converted bus, RV, or tractor-trailer.
Standard Operating Procedures	Set of stepwise written instructions that document a routine or repetitive activity followed by an organization to ensure that a specific task is performed the same way each time.
Sterilization	When a sterile surface/object is completely free of living microorganisms and viruses. Methods used in sterilization procedures include heat, ethylene oxide gas, hydrogen peroxide gas, plasma, ozone, and radiation.



# Section I: Introduction

## Profile

In geographical locations where diagnostic laboratory support is limited, infectious disease outbreaks such as the current COVID-19 pandemic can result in exceptionally high infection rates. The use of mobile laboratories can enhance the potential to detect, diagnose, and report any emerging infectious disease outbreak and inform public health authorities so that they can respond appropriately to limit and prevent potential pathogen transmission.

Several resources were used to create this manual, National Health Vision Pakistan 2016–25, provincial health strategies, National Biosafety and Biosecurity Policy,<sup>3</sup> and the World Health Organization (WHO) Laboratory biosafety manual.<sup>4</sup>

## Purpose

The purpose of this manual is to provide standardized guidelines on biosafety and biosecurity of mobile BSL-2 laboratories to enable and ensure maximum protection and monitoring against physical, biological, and environmental hazards.

## Scope

The manual is designed to:

- Provide a safe working environment for mobile laboratory staff and related personnel
- Protect mobile laboratory staff from possible biological hazards
- Strengthen mobile laboratories' staff capacity in biosafety and biosecurity
- Minimize physical and biological risks in operating mobile BSL-2 laboratories

## Responsibilities

### a) Mobile Laboratory Manager

- Provide appropriate training to perform laboratory procedures competently
- Develop laboratory-specific standard operating procedures (SOPs) for biosafety and biosecurity
- Maintain engineering controls covering biosafety cabinets (BSCs), directional air flow, and high-efficiency particulate air (HEPA) adequacy to control and minimize exposure to biohazardous agents
- Always provide mobile BSL-2 laboratory staff with personal protective equipment
- Ensure that occupational health precautions for laboratory personnel are universally practiced including vaccination and routine medical surveillance
- Notify the biosafety officer or safety coordinator of any physical and biological incident(s), (physical accidents, spills, or mishaps) in the mobile BSL-2 laboratory that may result in exposure to laboratory staff, the general public, or environmental discharge
- Ensure that biological wastes are handled and disposed of in accordance with local laws and standard good practices

---

<sup>3</sup> National Biosafety and Biosecurity Policy, 2018; available at <https://www.nih.org.pk/national-laboratory-biosafety-biosecurity-policy/> accessed on May 1, 2022

<sup>4</sup> WHO Laboratory biosafety manual, 4th edition, December 21, 2020

All employees working in the lab will be vaccinated. No employee will be trained to work in the lab without the express permission of Prof. Dr. Aamer Ikram, executive director, National Institute of Health (NIH) Pakistan. New SOPs and protocols must be approved by Dr. Ikram before initiation. Changes to SOPs and protocols that include new agents or risks or change the basis of Institutional Biosafety Committee (IBC)-approved protocols must be submitted for review by the IBC Biosafety Pakistan Agricultural Research Council.

Current SOPs and protocols will be reviewed and/or revised by Dr. Ikram every six months.

## **b) Provincial Mobile BSL-2 Laboratory Coordinator**

- Coordinate and ensure operations of all matters related to the mobile BSL-2 laboratory
- Ensure capacity building of all technical and support staff on operations, security, biosafety, biosecurity, and data management
- Coordinate and administer the bio risk management system for the mobile BSL-2 laboratory
- Periodically conduct risk assessments on the handling of infectious materials in the mobile BSL-2 laboratory
- Keep track of all biological samples and items through the mobile laboratory enterprise solution
- Conduct regular safety and security inspections
- Stay current on latest information and details related to the safe and secure handling of biological materials in the mobile BSL-2 laboratory setting
- Provide onsite and off-site guidance and information on biosafety, biosecurity, and operations of mobile BSL-2 laboratories

# Section II: Protocols for Operations, Security, and Response Plan of Mobile Biosafety Level 2 Laboratory

## Defining the RISK

The Mobile BSL-2 Laboratories may encounter risks during their operations, which may encompass breach in biological and physical security. Such risks may render them susceptible to a high degree of vulnerability. In response, risk assessments will be periodically carried out to ensure that the laboratory has mitigation processes in place to encounter any incidents.

This document provides the response to an emergency affecting staff, equipment, or the Mobile BSL-2 Laboratory or its operations. By having an emergency response plan the teams will minimize the impact of an emergency or disaster. It is important for all involved response entities to coordinate and plan their activities in advance.

Recognizing that emergencies often require unilateral as well as joint action, an incident management team (IMT), described below, will work in collaboration with the district and provincial Departments of Health, local law enforcement agencies, and health institutions where and when required and applicable. The Security Management Plan is provided in Annex I.

## Response Management

Incident management refers to a set of practices, processes, and solutions that enable teams to detect, investigate, and respond to incidents. It is a critical element for businesses of all sizes and a requirement for meeting most data compliance standards. The incident management uses a chain of command that is based on function, and not title.

The Five Steps of Incident Resolution to be managed by the incident management committee include the following:

1. Incident Identification, Logging, and Categorization
2. Incident Notification and Escalation
3. Investigation and Diagnosis
4. Resolution and Recovery
5. Incident Closure

In case of any emergency, or physical or biological incident, the following members of the incident management committee should be contacted immediately:

Table 1: Incident Management Committee

Sr. No	Lab	Focal Person	Designation	Lab Location	Contact details	Email ID
1	Lab-1- NIH	Dr. Muhammad Salman	Chief Public Health Lab Division Officer	Pakistan National Institute of Health, Park Road, Chak Shahzad, Islamabad	(+92) 333-538-4248; (+92) 051-925-5238	<a href="mailto:salman14m@gmail.com">salman14m@gmail.com</a>
2		Dr. Fahim Tahir	Principal Scientific Officer		(+92) 333-570-9061; (+92) 051-925-5238	<a href="mailto:faheemtahir2000@gmail.com">faheemtahir2000@gmail.com</a>
3		Mr. Firdous Khan	Senior Engineer		(+92) 051-925-5211; (+92) 300-530-9996	<a href="mailto:bpdnih@yahoo.com">bpdnih@yahoo.com</a>
4			Operations Security and Response Officer			
5	Lab-2 - Punjab	Dr. Hasnain	Lab In Charge Punjab Aids Control Program (PACP)	Institute of Public Health, Punjab AIDS Control Program, Lahore  06 Birdwood Road, Jubilee Town Lahore	0333-4591434	<a href="mailto:hasnain_javed@hotmail.com">hasnain_javed@hotmail.com</a>
6	Lab-3- Khyber Pakhtunkhwa	Prof. Dr. Jawad Ahmed	Dean Basic Medical Science	Khyber Medical University Peshawar	0300-5995439	<a href="mailto:j62ahmed@yahoo.com">j62ahmed@yahoo.com</a>
7	Lab-4- Sindh	Dr. Saeed Khan	Professor and Head of Molecular Pathology DUHS	DOW University of Health Sciences, OJHA CAMPUS & HOSPITAL: Main, University Road, KDA Scheme 33, Gulzar-e-Hijri, DUHS, Karachi	0333-2276556	<a href="mailto:saeed.khan@duhs.edu.pk">saeed.khan@duhs.edu.pk</a>
8		Mr. Noor Sade	Focal Person Public Health Reference Laboratory	Provincial Public Health Reference Lab, Fatima Jinnah General and Chest Hospital, Western Bypass Brewery Road, Quetta	0333-2227406	<a href="mailto:neemlevanai@gmail.com">neemlevanai@gmail.com</a>

Table 2: List of drivers and contact details (temporary for two months)

Sr No.	Vehicle No.	Engine No.	Chassis No.	Driver Name	License No.	Contact No.
1	E-3401	GH8521276AIP	PCZZ30D4M T028776	Munir Ahmed	22107	0300-2554433
2	E-32 01	GH8519 872AIP	PCZZ30D4M T028647	Hidayat Ullah	112000007004.00	0346-6505156
3	E-3701	GH8521 264AIP	PCZZ30D8M T028778	Bashir Ahmed	113353	0345-5381279
4	APF	GH8543224AIP	PCZXYOD9NT031385	Sajjad Hussain	2855	0300-8837294

## Incident Management and Reporting

Any physical or biological event must be reported to the notified and provincial lab focal person and Operations, Security and Response Plan Officer (OSRO) either through a telephone call or online on the Enterprise Lab Solution home page; click on the “Report an Incident, Near-miss, or Safety Concern” link.

During the field deployment, the representative of local district health administration coordinating with local law enforcement agencies (LEAs) will be the primary contact person, and the secondary contact point will be the provincial lab focal persons and OSRO (a security official from the project’s Business Risk Department (BRD) team). In case of movement (which will be need based), their district offices will be contacted using the contact information provided. A detailed incident management plan can be accessed in Annex 2.

The Security Management Plan lays down the deployment procedure of mobile labs in coordination with local LEAs. The labs are recommended to be parked and operate within a government premises/hospital in the field. Further, closed-circuit television (CCTV) for remote viewing from the security control room at NIH/GHSC-PSM offices will be another alternative to identify potential problems within and surrounding the lab. The cell phone, however, is still the most agile way to communicate.

## Accidents

Accidents in or on Mobile BSL-2 Laboratories can be attributed to unintended breaches in biosafety, biosecurity protocols, accidents on the road, and an attack on the Mobile BSL-2 Laboratory, which may require medical attention.

Following is the list of hospitals that should be contacted, and the affected personnel may be transported on site while following due standard operating procedures in collaboration with 1122 Emergency Services or Edhi Ambulance Services.

## Laboratory I: National Institute of Health, Islamabad

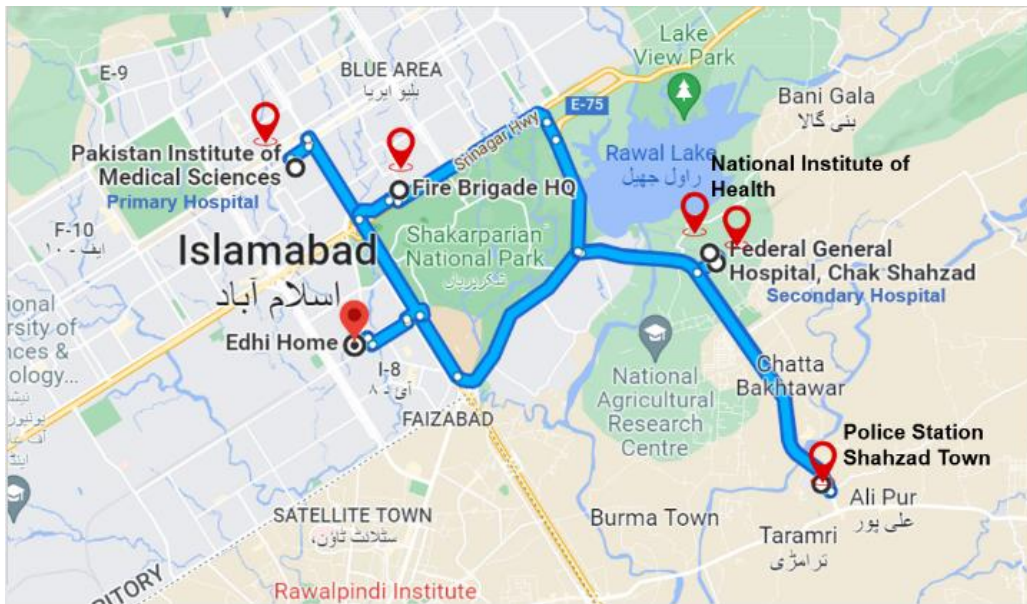


Figure 1: Islamabad Map with response areas

### Primary Hospital

Pakistan Institute of Medical Sciences, Islamabad

Hours of Operation: 24 hours

Address: Ibn-e-Sina Rd, G-8/3, Islamabad

Phone Number(s): 9261170-89

Email: edpims@pims.gov.pk

### Secondary Hospital

Federal Government Services Hospital (Poly Clinic Hospital)

Hours of Operation: 24 hours

Address: Polyclinic, Service Road, G-6/1, Islamabad

Phone Number: +92-51-9214965

### Other Contact Details:

#### Police

Shahzad Town Police Station

Telephone: +92- 51- (051) 9247444

Hours of Operation: 24 hours

Address: Park Road, Islamabad

#### Fire Brigade

Fire Brigade HQ, Islamabad, +92-51-9252842. 1122, 16

Hours of Operation: 24 hours Address: G-7/1, Khayaban-e – Suhrwardy, Islamabad

#### Ambulance Services

Edhi Foundation +92-51-2522205, 115

Hours of Operation: 24 hours Address: Edhi Center, H-8/1, Islamabad

## Laboratory 2: Institute of Public Health, Lahore, Punjab

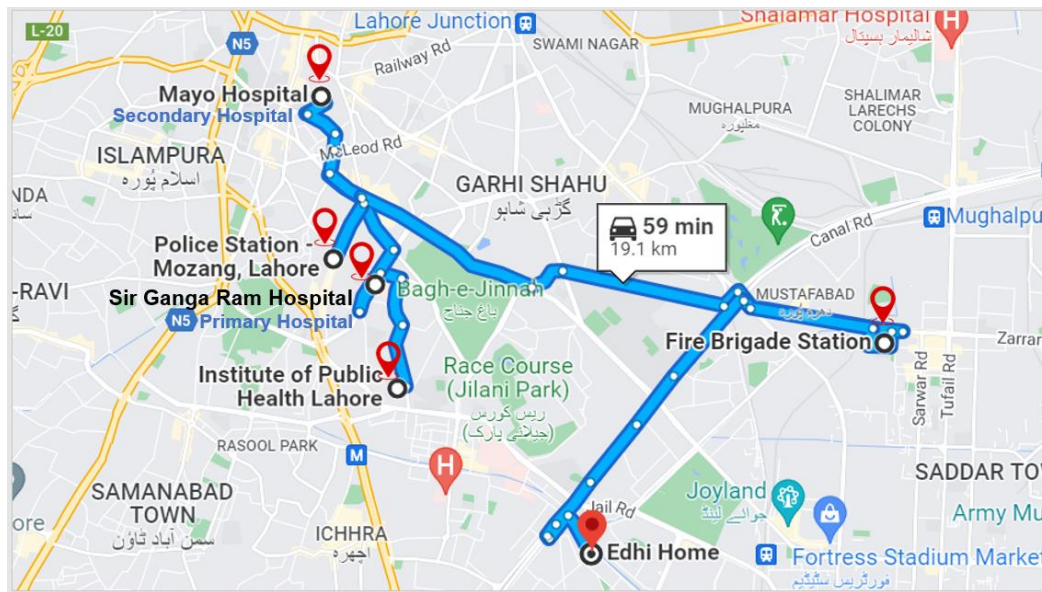


Figure 2: Map of Lahore, Punjab with response areas

### Primary Hospital

Sir Ganga Ram Hospital

Hours of Operation: 24 Hours

Address: Shara-I-Fatima Jinnah, Queen's Road, Jubilee Town, Lahore

Phone Number: +92-42-99200572

### Secondary Hospital

Mayo Hospital

Hours of Operation: 24 hours

Address: Hospital Road, Anarkali Bazaar, Lahore

Phone Number: +92-42-99211125

### Other Contact Details

#### Police

Mozang Police Station

Telephone: +92- 42 - 37320565

Hours of Operation: 24 hours

Address: Mozang Chungi, Lahore

#### Fire Brigade

Address: Band Rd, Tariq Colony, Sodawal Gulshan-e-Ravi, Lahore

Hours of Operation: 24 hours

Contact Number: 1122

#### Ambulance Services

Rescue 1122

Contact Number: 1122

Edhi Foundation +92-42-37806664, 115

Hours of Operation: 24 hours

Address: Edhi Center, 17 A, Main Boulevard Allama Iqbal Town, Lahore



## Laboratory 3: DOW University Ojha Campus, Karachi, Sindh

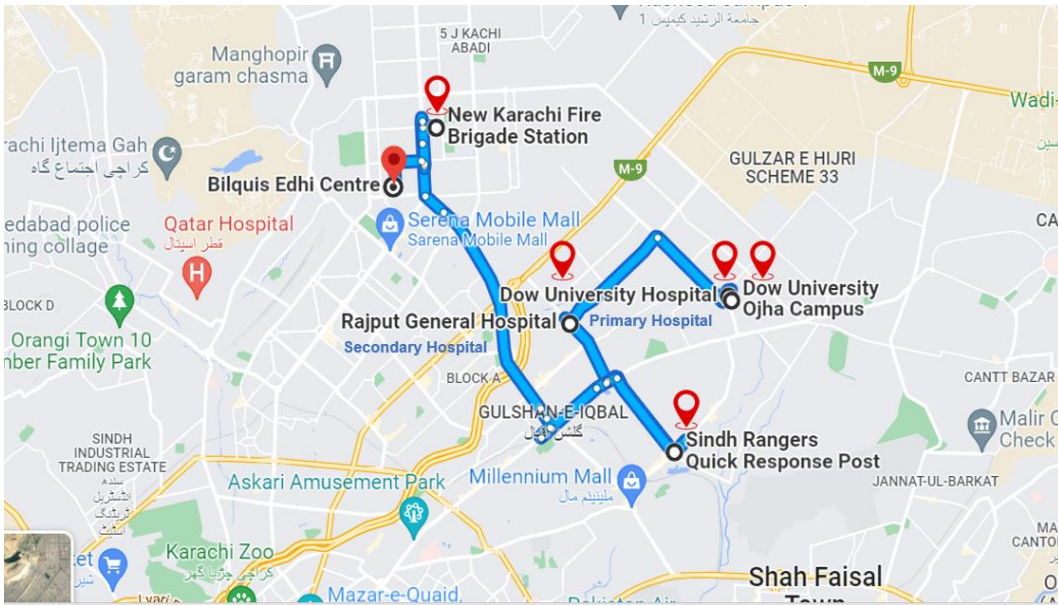


Figure 3: Map of Karachi, Sindh with response areas

### Primary Hospital

Dow University Hospital

Hours of Operation: 24 hours

Address: Gulzar-e-Hijri Scheme-33, Suparco Road, Karachi

Phone: +92 21 38771111

### Secondary Hospital

Rajput General Hospital

Hours of Operation: 24 hours

Address: ZC-2, Block 4, Gulshan-e-Iqbal, Abul Hasan Isphani Road, Karachi

Phone: 92-21-34979403, More Number: 92-21-34979403

### Other Contact Details

#### Sindh Rangers Quick Response Post

Emergency Contact Number: 1101

#### Fire Brigade

New Karachi Fire Brigade Station

Hours of Operation: 24 hours

Address: Sector-II-I Sector III North Karachi Twp, Karachi, Karachi City, Sindh

Phone: (021) 36974030

#### Ambulance Services

Edhi Foundation 115

Hours of Operation: 24 hours

Address: Bilquis Edhi Center, Karachi

Chippa Ambulance Services

Hours of Operation: 24 hours

Address: Shahrah-e-Usman, Sector II-K Sector III L North Karachi Twp, Karachi

Phone: +92-21-111-92-1020



## Laboratory 4: Khyber Medical University, Public Health Reference Lab, Peshawar, Khyber Pakhtunkhwa

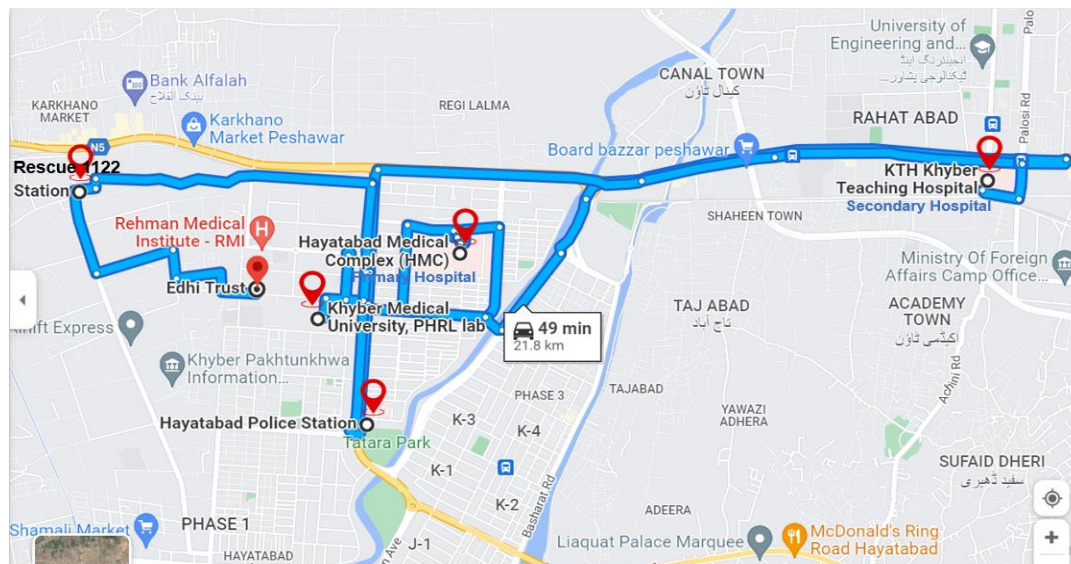


Figure 4: Map of Peshawar, Khyber Pakhtunkhwa with response areas

### Primary Hospital

Hayatabad Medical Complex

Hours of Operation: 24 hours

Address: Phase-4 Phase 4 Hayatabad, Peshawar, Khyber Pakhtunkhwa

Phone Number(s): (091) 9217140

### Secondary Hospital

KTH Khyber Teaching Hospital

Hours of Operation: 24 hours

Address: University Rd, Rahat Abad, Peshawar

Phone Number: (091) 9224400

### Other Contact Details

#### Police

Hayatabad Police Station

Telephone: (091) 9217333

Hours of Operation: 24 hours

Address: Ring Rd, Phase-4 Phase 4 Hayatabad, Peshawar, Khyber Pakhtunkhwa

#### Fire Brigade

Rescue 1122 station, Hayatabad Peshawar

Hours of Operation: 24 hours

Telephone: 1122

#### Ambulance Services

Rescue 1122 station, Hayatabad Peshawar

Hours of Operation: 24 hours

Telephone: 1122

Edhi Trust Phase 5, Hayatabad Peshawar

Hours of Operation: 24 hours

Telephone: (091) 5892769/ 115

## **Incident Management**

The designated national and provincial OSROs of Mobile BSL-2 Laboratory will notify the head of the laboratory services in each province, office of the director general health services, and the chief public health laboratory at NIH, Islamabad. The OSRO will also investigate reported incidents and provide a written critique of the incident. Details are provided in Annexes I-5.

## Section III: Mobile BSL-2 Laboratory

To strengthen Pakistan's capacity to detect public health events due to infectious diseases, including COVID-19, USAID has contributed to the procurement of four Mobile Biosafety Level 2 Laboratories (BSL-2) for federal and provincial governments and regions. These include one mobile laboratory for Islamabad Capital Territory (ICT) [to cover ICT, Azad State of Jammu & Kashmir (AJK) and Gilgit Baltistan (GB)], Khyber Pakhtunkhwa (KP), Punjab, and Sindh (to cover Balochistan), respectively. These laboratories will be instrumental in diagnosing public health events, especially in remote and hard-to-reach, areas as well as during outbreaks, epidemics, pandemics, and natural disasters.

### Salient Features of Mobile BSL-2 Laboratory

- Baker SterilGARD e3 Class II, Type A2 SG404, complete with Stand, Flexair, and UV
- UPS for Biosafety cabinets - 2KVA
- EL450 - Fridge Freezer combo upright 2C TO 8C/-10C to -25C racks included
- Tianlong LIBEX Extractor
- GeneXpert
- Realtime PCR Machine 4 Channels
- TOPAIR PCR unit with UV light and HEPA filter - 3ft
- 3781L - MLS Floorstanding Panasonic Autoclave
- C15-24.2PR - Refrigerated High-Speed Micro Centrifuge with Timer, Max 15000rpm, Temperature Range: -20°C to 40°C
- C6-4.100CP - Advanced Multi-Purpose Clinical Centrifuge with Timer, Max 6000rpm
- CFR-8.50 - Fixed Angle Aluminum Rotor with Stainless Steel Adapters, Max Speed: 5000rpm, Max RCF: 3460xg
- Vortex Mixer
- ELISA Plate Reader 96 Well 405, 450, 492,620nm
- Elisa Microplate washer
- H3 - Horizontal Electrophoresis ET-H3 with 300w power supply
- DNA/RNA Quantification System - Biobase Micro-Volume UV Vis Spectrophotometer
- Hands-Free Disinfection Station

The complete layout plan is presented in Annex 6.

### Security

For security, all labs will feature the following security and safety measures:

- All authorized personnel of mobile BSL-2 laboratory will have access only through biometric
- CCTV in each room and two external cameras
- Two-zone fire alarm system tied into control system
- Intercom system (three-station system, one installed in each room as well as one at the main entrance door)
- Multi-zone burglar alarm system, including motion sensors for each room, keypad for arming and disarming, siren, emergency panic button
- BSL-2 sensors installed in enclosures that can withstand the chemicals associated with room decontamination
- Burglar bars on windows
- Access control system with keycard access (upon arrival to the destination city/province); the NIH Pakistan will change the default vendor security codes

- All internal doors fitted with red (open door) and green lights to ensure proper door closure and airflow
- Satellite tracking system on each laboratory, trailer/power bank that are active 24/7/365
- Professionally trained security guards and drivers
- SOPs easily accessible in each laboratory

## Preventative Maintenance

The laboratory manufacturer’s engineering team will visit three times in the first year (4, 8, and 12 months) and twice (6 and 12 months) in the next two years to spend two to three days onsite for preventive maintenance of mobile laboratories. This would include facility annual service and equipment re-certification, refresher training for users, certification of biosafety cabinets, and performance verification on the BSL-2 labs.

Table 3: List of biomedical engineers and contact details

Sr. No	Name	Vendor	Designation	Address	Contact number
1	Mr. Gregers Chalker	Air Filter Maintenance Services International (PTY) Ltd.	CEO	30 Summit Road, Blue Hills, Midrand, 2162	(27) 011-462-0120
2	Mr. John David Rautenbach				
3	Mr. William Mmoni Kau				
4	Mr. Professor Nyoni				
5	Mr. Andrew Richard Darvall				
6	Mr. Malibongwe Makhanya				
7	Mr. Marc De Villiers				
8	Mr. Jacobus Frederick Johannes Willem Fisher				

## Section IV: Biological Risk Assessment

Methodology for identifying hazards and assessing risks that come with biological agents and toxins, considering the effectiveness of any existing safeguards, and determining if the risks are acceptable (Figure below).

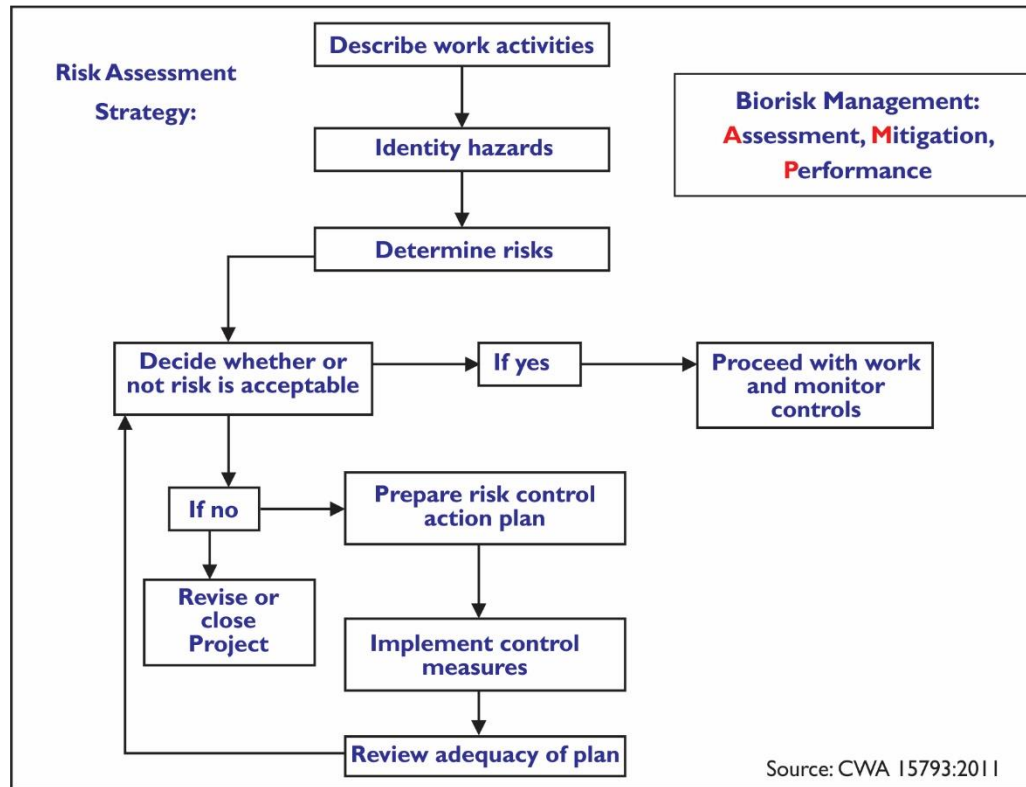


Figure 5: Risk Assessment Strategy

### Hazard Identification

- Agent's hazardous characteristics
- Laboratory procedures with hazardous characteristics
- Workplace hazards, including safety equipment and facility controls

### Risk Assessment

A risk assessment is a procedure that examines a process or scenario to identify the possibility and effects of a certain undesirable occurrence.

### Risk Characterization

The features of the agent and the laboratory techniques are used to characterize risk in the laboratory.

### Risk Evaluation

Risk evaluation is the subjective process of determining whether a risk is high or low, and whether it is acceptable. It is a crucial step between risk characterization and taking proactive actions to reduce risk.

## Risk Reduction

Hierarchy of risk mitigation is dependent upon the following:

- Elimination of the hazard
- Substitution of the hazard with a less hazardous version
- Engineering controls
- Administrative controls
- Personal protective equipment

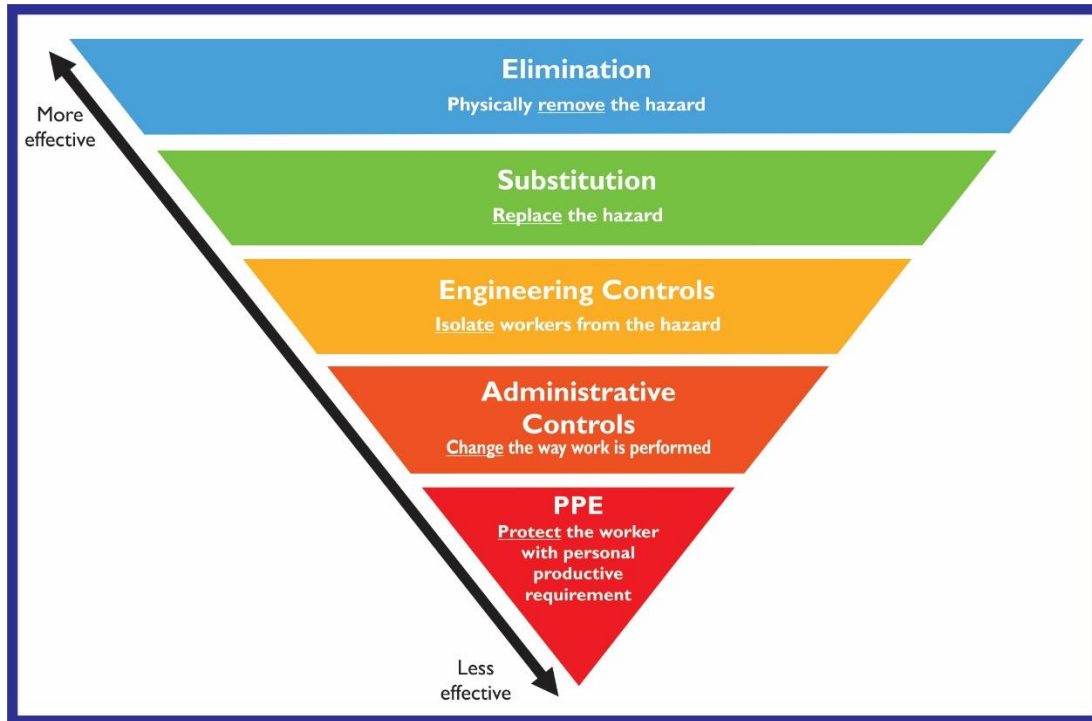


Figure 6: Triangle of hierarchy

Security mitigation is generally broken up into the following pillars:

- Transportation security
- Material control and inventory
- Information security
- Personnel management
- Physical security

## Risk Communication

Risk communication is the responsibility of laboratory managers, biosafety officers, or safety coordinators to guarantee the safety of the workers and lab environment. They will:

- Use signs, films, posters, and announcements to introduce warning systems in the lab
- Conduct monthly meetings/lectures with staff/employees at the laboratory workstation, through email notifications
- Clearly define communication protocols for use in an incident or accident

# Section V: Administrative Control

- a) Standard Operation Procedure Compliance
- b) Occupational Health
- c) Training
- d) Mechanisms for Continuous Improvement

## Standard Operating Procedures

SOPs are developed to establish a consistent, repeatable method for performing common, repetitive tasks. The set approach and methods presented in the SOPs ultimately enhance the efficiency and safety of the procedure. SOPs should be:

- Regularly updated
- Easy to access by laboratory personnel
- In legible writing and easily readable
- Reviewed after every change in the staff, equipment, or procedures

SOPs for autoclave are provide in Annex 12.

## Occupational Health/Medical Surveillance

The following are components of any effective institutional occupational health program:

- Preplacement medical evaluations
- Periodic medical evaluations
- Immunization program for the laboratory staff (vaccines)
- Medical surveillance
- Occupational health support
- Incident reporting
- Pre- and post-exposure communications
- Post-exposure follow-up care and testing

## Training

Avoiding laboratory-acquired diseases, injuries, and accidents requires a safety-conscious staff that is well-informed about detecting and controlling laboratory hazards. That is why biosafety measures require ongoing in-service training. The NIH plans to formally engage Pakistan Biological Safety Association (PBSA) for trainings and periodic oversight. The designated mobile BSL-2 laboratory staff are required to receive biosafety and biosecurity training as part of their onboarding process. The concerned staff will be given access to the Mobile Biosafety & Biosecurity Manual along with the defined SOPs.

Training and training aids, as well as documentation of these trainings, are the responsibility of the designated Provincial Mobile BSL-2 Laboratory safety coordinator at NIH Islamabad. All personnel who work in the laboratory will receive adequate instruction from their supervisor before beginning work. Some trainings will be provided annually. Each lab will require different trainings. The minimum requirements for qualification to work in the mobile BSL-2 lab are:

1. Annual Bloodborne Pathogen Training.
2. Annual Biosafety Level 2 Training.
3. Annual Laboratory Specific Training (risks associated with the hazards/agents used in the lab, SOPs, Spill and Exposure Procedures).

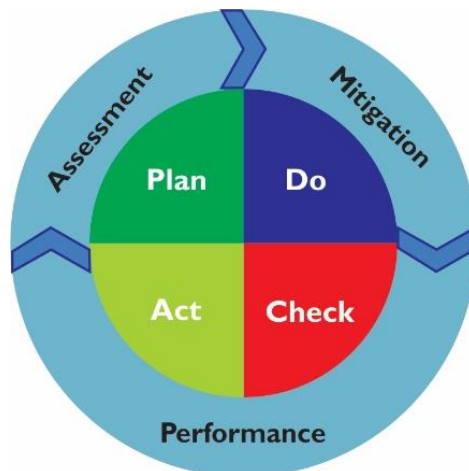
4. Shipping Training: Training is required to commercially transport infectious materials, as well as shipping anything on dry ice. Contact Environmental Health and Safety to schedule a training class.
5. Annual Review of this Manual.

The training program will include the following:

- Inhalation risks while using loops, streaking agar plates, pipetting, producing smears, opening cultures plates, obtaining blood/serum samples, centrifuging, and other procedures
- Ingestion risks when working with specimens, smears, and cultures
- Risks of accidental percutaneous inoculation due to the use of infectious syringes and needles
- Emergency response procedures in accordance with proposed SOPs
- Training in the use of installed equipment in the mobile BSL-2 laboratories
- Training on protocols for Operations, Security, and Response Plan

## Mechanisms for Continuous Improvement

An effective management system approach is based on the idea of continuous improvement, which is accomplished through a cycle of planning, implementing, reviewing, and refining the processes and activities that an organization takes to achieve its objectives. The PDCA (Plan-Do-Check-Act) concept is a bio risk management method that supports the AMP (Assessment-Mitigation-Performance) Model (see figure below).



*Figure 7: Assessment Mitigation Performance Model*

Risk assessment for lab deployment will be carried out annually and when screening newly inducted lab staff, responding to any incident, including new equipment, and whenever required.



# Section VI: Work Practices

## Good Laboratory Practices

1. The laboratory supervisor is responsible for enforcing mobile laboratory policy control, safety, and access to the facility.
2. The Provincial Mobile BSL-2 Laboratory safety coordinator and laboratory supervisor are responsible for providing appropriate training for procedures to be conducted in the laboratory as per their assigned duties.
3. A biosafety manual is available and accessible to all the laboratory staff and with continuously reviewed and updated as required.
4. The biosafety manual will provide essential information to the lab staff about the control on procedures for the biohazardous material in use, and their decontamination methods.
5. Access to the Mobile BSL-2 Laboratory will be granted to the designated and trained mobile BSL-2 staff, provincial Mobile BSL-2 Laboratory safety coordinator by using keypad access or specific tags.
6. A biohazard signage (in Urdu and English language) will be posted at the entrance of the mobile laboratory with the following information as per the policy of the mobile laboratory:
  - a) No use of cell phones/smart phones/smart watches, etc., while in the mobile BSL-2 lab.
  - b) No animals or minors (persons under the age of 18) will be allowed to enter the lab at any time.
  - c) Food, medications, or cosmetics should not be brought into the lab for storage or later use. Food is stored outside in areas designated specifically for that purpose.
  - d) No open-toed shoes or sandals are allowed in the laboratory.
  - e) No bare legs or arms are allowed.
  - f) Personnel working with virus must wear a lab coat (or gown) with tight cuffs, safety glasses, or facemask, and two pairs of gloves. For work with high-risk agents transmissible by inhalation, personnel should wear an N95 respirator (see Section D.3.). Lab coats must be left in the lab. Upon entering the tissue culture facility, personnel must immediately don a gown or laboratory coat with long sleeves. Optional disposable sleeves with tight cuffs are available for personnel when using a lab coat with loose cuffs.
  - g) All skin defects such as cuts, abrasions, ulcers, areas of dermatitis, etc. should be covered with an occlusive bandage.
  - h) All procedures are to be performed carefully to minimize the creation of splashes or aerosols. Aerosols containing RG2/BSL-2 agents pose an increased risk of exposure to personnel. Solutions containing RG2/BSL-2 agents will be enclosed in capped containers during agitation (vortexing, shaking, centrifugation, etc.). If agitation is performed outside of a safety cabinet, two levels of containment are required (i.e., capped tube enclosed in plastic bag or Tupperware). After agitation, containers will be opened only in a biosafety cabinet to prevent exposure to personnel from aerosols. Human cells/tissue will be homogenized inside a biosafety cabinet. Centrifugation of hazardous materials must be performed using centrifuge safety caps or sealed rotors.
7. Gloves are required to be worn for protection of hands from hazardous biological material.
8. Proper donning and doffing of gloves are required to prevent self-contamination.
9. Wash hands after working with potentially infectious material and before exiting the laboratory.
10. Wear a head cover to prevent long hairs from contact hands, specimens, containers, and equipment.
11. Food and drink are not permitted in the mobile BSL-2 laboratory (eating, drinking, handling cosmetics, and contact lenses are prohibited).
12. Mouth pipetting is not allowed, and as such, use of mechanical or automated pipetting is recommended.

13. Safe handling of sharps, including needles, blades, broken glass, and sharp pipettes should be placed in puncture-resistant containers and not to be handled directly and as per policies developed for their treatment and disposal.
  - a) Avoid the use of needles and other sharps whenever possible. Use plastic alternatives to glass if available.
  - b) Minimize any contact with sharps by disposing or storing them immediately after use.
  - c) Needles must never be recapped, removed from the syringe, sheared, bent or broken.
  - d) Use a mechanical device to remove scalpel blades. Never use your fingers.
14. Avoid making splashes and aerosols while performing work in the laboratory.
15. Decontaminate laboratory benches before and after completing work, after any spills or splashes.
16. Include a proper pest management program for better and contained environment.
17. Provide controlled access to the working area when the laboratory is engaged in testing.
18. Biosafety cabinets are to be used when there are chances of production of aerosols when the following procedures are conducted:
  - a) Pipetting, centrifuging, grinding, blending, shaking, mixing, sonicating, opening containers.
19. Centrifugation should be done in an open laboratory with sealed rotors or safety cups with loading and unloading in the biosafety cabinet (BSC).
20. Laboratory equipment is routinely decontaminated, and after any spills, before repair, maintenance, or removal from the mobile BSL-2 laboratory.
21. Laboratory waste should be decontaminated before it leaves the laboratory (autoclave, chemical disinfection, or other validated decontamination method).

## Laboratory Aerosols

A significant amount of mobile BSL-2 laboratory procedures may account to produce biological aerosols. This may be hazardous to the health of laboratory workers and the environment. It is mandatory to comply with Good Laboratory Practices, which will minimize aerosol. Aerosol-generating procedures should be performed in BSC.

1. Apply respiratory protection as per risk assessment.
2. Whenever spill occurs, leave the mobile BSL-2 laboratory and allow any aerosol generated to settle down before conducting the spill management.
3. Procedures that can produce aerosols require specific precautions:
  - a) **Centrifugation**
    - Use safety cups whenever possible
    - Disinfect or clean weekly and after all spills or breakages
    - Lubricate O-rings and rotor threads weekly
    - Do not operate the centrifuge without the rotor perfectly balanced
  - b) **Pipetting**
    - Dispense liquid materials close to the tubes
    - Rinse with proper disinfectant before disposal
    - Remove pipettes carefully
  - c) **Syringe use**
    - Discharge liquids, avoiding air bubbles
  - d) **Inoculations**
    - Use of pre-sterilized/disposable loops is recommended
    - While using reusable loops, make sure to cool them before presenting them to any infectious agents

- e) **Decanting of liquids**
  - Carefully pour close to the vessel
- f) **Vortexing**
  - Perform vortexing should in a durable container with a tightly fitting cap
- g) **Blending**
  - Always operate the blender in a BSC; allow the aerosol to settle before opening the lids
- h) **Sonication**
  - It is advisable to operate the Sonicator in the BSC if infectious material is sonicated



# Section VII: Safety Equipment Primary and Secondary Containment

Laboratory coats, gowns, and uniforms are worn in the mobile BSL-2 laboratory working area. The PPEs to be removed before leaving the laboratory include the following.

- Safety glasses, goggles, face shields, masks
- Laboratory coats, gowns, uniforms
- Shoe covers

## Primary Containment

### Sequence for Donning Personal Protective Equipment (PPE)

**Donning PPE will use a clean to dirty sequence, as follows:**

**1. Gown**

- a) Make sure the gown fully covers from neck, chest, and arms to the end of wrists and up to the knees and is wrapped around the back
- b) Fasten the gown at the back of neck and waist

**2. Mask or Respirator**

- a) Fix elastic bands and secure them at the middle of the band and neck
- b) Set up the nose piece properly
- c) Ensure a snug fit to the face and under the chin
- d) Use a fit test if required

**3. Face shield or Goggles**

- a) Wear over eyes and face and adjust

**4. Gloves**

- a) Extend gloves over to cover wrist and gown arms
- b) As per the risk assessment, wear double gloves

**Note:**

1. Hands should be kept away from the face
2. Prevent touching surfaces
3. Change the glove(s) when torn or profoundly contaminated
4. Perform a hand rub as required (use sanitizer)

### Sequence for Removing PPE

Removing PPE will use a dirty to clean sequence, as follows:

**1. Gloves**

- a) Outside surfaces of gloves are contaminated
- b) Immediately wash your hands or use hand sanitizer if hands get contaminated during removal of gloves
- c) Use a glove-in-glove technique or beak method for doffing of gloves
- d) Discard gloves in a biohazard waste bag





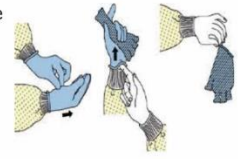





SEQUENCE FOR <b>PUTTING ON</b> PERSONAL PROTECTIVE EQUIPMENT (PPE)	SEQUENCE FOR <b>REMOVING</b> PERSONAL PROTECTIVE EQUIPMENT (PPE)
<p>The type of PPE used will vary based on the level of precautions required, such as standard and contact, droplet or airborne infection isolation precautions. The procedure for putting on and removing PPE should be tailored to the specific type of PPE.</p> <p><b>1. GOWN</b></p> <ul style="list-style-type: none"> <li>Fully cover torso from neck to knees, arms to end of wrists, and wrap around the back</li> <li>Fasten in back of neck and waist</li> </ul>  <p><b>2. MASK OR RESPIRATOR</b></p> <ul style="list-style-type: none"> <li>Secure ties or elastic bands at middle of head and neck</li> <li>Fit flexible band to nose bridge.</li> <li>Fit snug to face and below chin</li> <li>Fit check respirator</li> </ul>  <p><b>3. GOGGLES OR FACE SHIELD</b></p> <ul style="list-style-type: none"> <li>Place over face and eyes and adjust to fit</li> </ul>  <p><b>4. GLOVES</b></p> <ul style="list-style-type: none"> <li>Extend to cover wrist of isolation gown</li> </ul> 	<p>Except for respirator, remove PPE at doorway on in anteroom, Remove respirator after leaving patient room and closing door.</p> <p><b>1. GLOVES</b></p> <ul style="list-style-type: none"> <li>Outside of gloves is contaminated!</li> <li>Grasp outside of glove with opposite gloved hand; peel off</li> <li>Hold removed glove in gloved hand</li> <li>Slide fingers of ungloved hand under remaining glove at wrist</li> <li>Peel glove off over first glovet</li> <li>Discard gloves in waste container</li> </ul>  <p><b>2. GOGGLES OF FACE SHIELD</b></p> <ul style="list-style-type: none"> <li>Outside of goggles or face shield is contaminated!</li> <li>To remove, handle by head or ear pieces</li> <li>Place in designated receptacle for reprocessing or in waste container</li> </ul>  <p><b>3. GOWN</b></p> <ul style="list-style-type: none"> <li>Gown front sleeves are contaminated!</li> <li>Unfasten ties</li> <li>Pull away from neck and shoulders, touching inside of gown only</li> <li>Turn gown inside out</li> <li>Fold or roll into a bundle and discard</li> </ul>  <p><b>4. MASK OR RESPIRATOR</b></p> <ul style="list-style-type: none"> <li>Front of mask/respirator is contaminated - DO NOT TOUCH!</li> <li>Grasp bottom, then top ties or elastics and remove</li> <li>Discard in waste container</li> </ul> 
<p><b>USE SAFE WORK PRACTICES TO PROTECT YOURSELF AND LIMIT THE SPREAD OF CONTAMINATION</b></p> <ul style="list-style-type: none"> <li>Keep hands away from face</li> <li>Limit surfaces touched</li> <li>Change gloves when torn or heavily contaminated</li> <li>Perform hand hygiene</li> </ul> 	<p><b>PERFORM HAND HYGIENE BETWEEN STEPS IF HANDS BECOME CONTAMINATED AND IMMEDIATELY AFTER REMOVING ALL PPE</b></p> 

Figure 8: Sequence for donning and doffing of PPE

SOPs for laundry can be found in Annex 14.

**1. Goggles or Face shield**

- a. External surface of goggles or face shield are contaminated
- b. Remove face shield or goggles from the back by lifting head band slowly without touching the outer surface of face shield or goggles
- c. If the item is reusable, place it in the selected container for reusing
- d. Discard in a waste bag

**2. Gown**

- a. Front of gown and sleeves are also contaminated
- b. Immediately wash your hands or use hand sanitizer if hands get contaminated during removal of gown
- c. Touch inside of gown only, and take gown away from the body
- d. Wrap the gown inside out
- e. Discard in a biohazard waste bag

**3. N95 mask or Respirator**

- a. DO NOT TOUCH the front of the mask/respirator, as it may be contaminated
- b. Immediately sanitize and wash your hands, after removing mask or respirator

- c. Grasp the lowermost ties of the respirator or mask, and then the one at the top, removing them without touching the front of the face mask or respirator
- d. Discard in a biohazard waste bag or container

**Note:**

1. Wash hands immediately after taking off all PPE
2. Also perform hand hygiene between these steps to avoid self-contamination

## **Secondary Containment**

1. Change clothes in the designated changing area.
2. Always wash hands using the sink near the exit door.
3. BSCs are located at the end of the working area to avoid any fluctuations of the room air supply and exhaust.
4. BSCs are certified annually, and after movement of the mobile laboratory from one location to another.
5. Vacuum lines, if in use, are protected with liquid disinfectant traps and inline HEPA filters.
6. The mobile laboratory design, operations, and procedures are verified and documented before operation and tested annually or after any major modification.





# Section VIII: Biological Safety Cabinets

## Classification

BSCs are essential for biological agent containment and safe handling. They're made to protect people, products, and the environment by using good laboratory and microbiological practices and procedures. In practice, there are three basic categories of BSCs. Class II is further subdivided into subtypes to match the laboratory's safe working environment.

- Class I
- Class II
- Class III

The BSCs installed in the mobile BSL-2 laboratory belong to Class II biosafety type. Details are provided in the table below.

Table 4: Classification of Class II Biosafety Cabinets

Classification Class II Biosafety Cabinets		
Type A	Type B	Type C
A 1	B 1	C 1
A 2	B 2	-

## Biological Safety Cabinets

- Baker SterilGARD e3 Class II, Type A2 SG404, complete with Stand, Flexair, and UV
- Field Certification details are as per NSF/ANSI 49 standard and provided in Annex 11

### Class I Biological Safety Cabinet

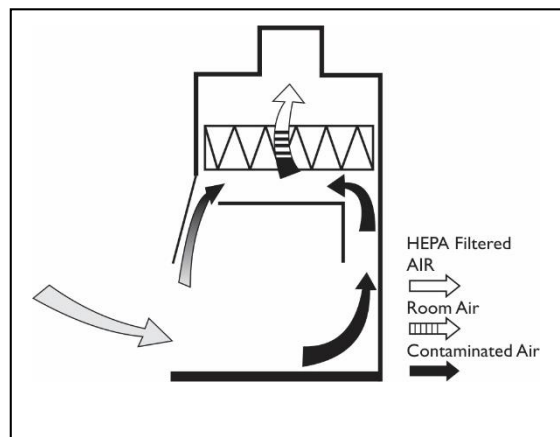


Figure 9: Class I Biological Safety Cabinet

## Class II Biological Safety Cabinets

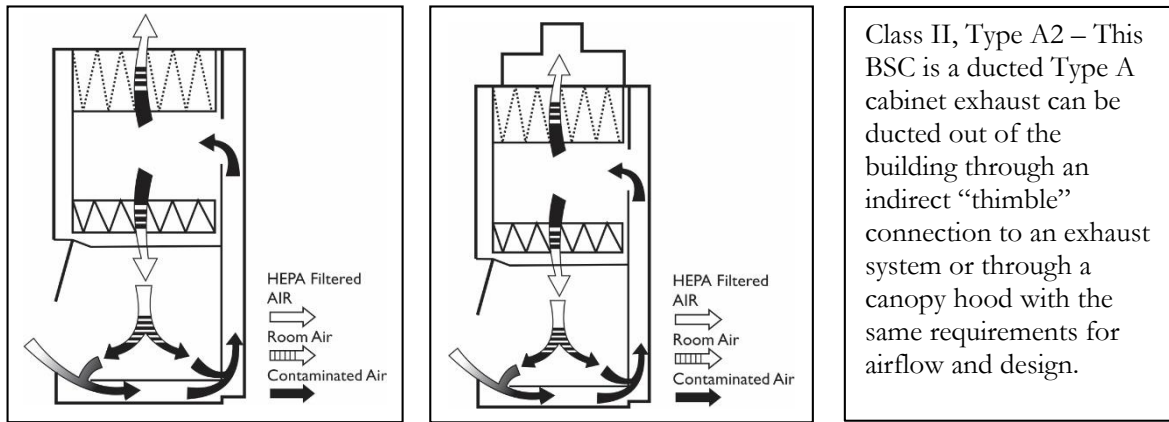


Figure 10: Class II Biological Safety Cabinets

## Class II, Type B2

This BSC is a total-exhaust cabinet; no air is recirculated within it. This cabinet provides primary biological and chemical containment. All air entering this cabinet is exhausted and passes through a HEPA filter before discharge to the outside.

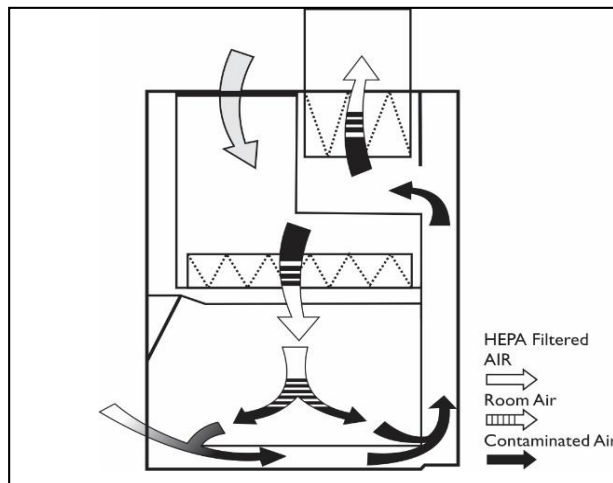


Figure 11: Class II, Type B2

## Operation within a Class II Biosafety Cabinet

BSCs are the most common type of containment for pathogenic pathogens. Biosafety cabinets use laminar airflow and HEPA filtration to keep pathogens out of the air in the BSC. The air curtain formed at the front of the cabinet is delicate, moving at only 100 lfpm downward and inward. A BSC should be placed away from heavy human traffic areas, air supply ducts, entrances/exits, and laboratory equipment since the air curtain generated at the front of the cabinet can be readily disturbed.

### Operational Use of Biosafety Cabinet

#### Before starting work:

- Check alarms, pressure gauges, and other indicators for any changes
- Shut off ultraviolet (UV) light if installed
- Turn the cabinet to life; let it run for 3–5 minutes to purge
- Disinfect work surface with 70 percent ethanol
- Place every item inside related to the work before starting work. Before placing items inside, wipe their outer surfaces with disinfectant

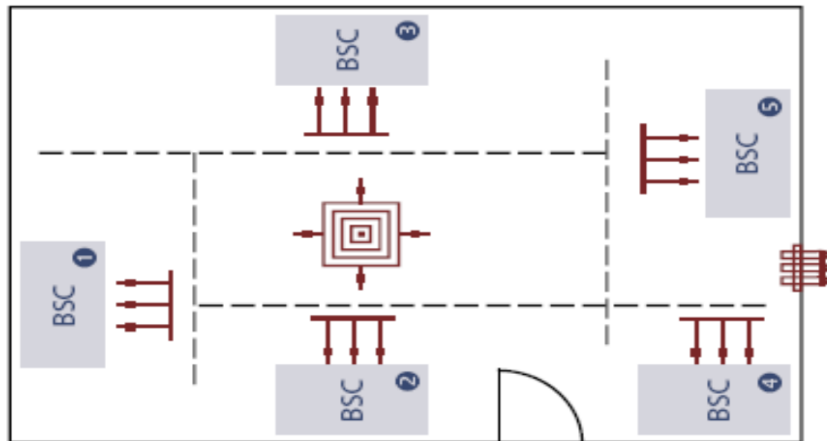


Figure 12: Operational diagram of Biosafety Cabinet

#### During work:

- Airflow disruption can affect the protection level offered by BSC
- BSC should be free of clutter
- Keep front and rear intake grills free of any objects or papers
- Limit human traffic during BSC operation
- Keep lab door closed and place BSC away from the opening and closing door
- Keep arms straight; avoid sweeping motions when working inside BSC
- Change gloves when moving in and out of the BSC while working with infectious materials
- Keep all items inside the work area almost 4 inches from the front sash
- Work from clean to dirty area and keep clean items one foot from aerosol-generating procedures to prevent cross-contamination
- Place centrifuge in the back to avoid any turbulence and stop other work during its working
- Bunsen burners are not allowed in the BSC, as they disrupt the laminar airflow within the cabinet
- Clean up all spills in the BSC immediately. Allow the cabinet to run for 3–5 minutes to purge before starting work again

#### After completion of work:

- Remove used gloves by approved methods (glove in glove or beaking)
- Don a fresh pair of gloves
- Disinfect all items before removing them from the cabinet
- After removal of all materials, wipe down the interior surface of BSC with appropriate disinfectant
- Remove gloves and wash hands after completing work

## Certification

NSF/ANSI 49-2019 is a standard for Class II BSCs that provides an independent standard for BSC design, manufacturing, and testing. This standard covers all Class II cabinet types (Types A1, A2, B1, B2, C1) and includes standards:

- a. Design/construction
- b. Performance
- c. Suggestions for installation
- d. Techniques of disinfection

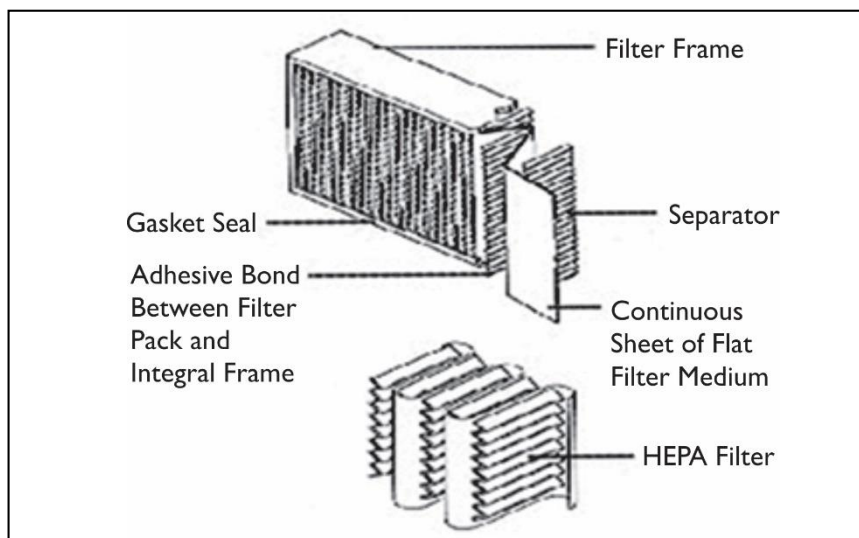
Class II BSCs are main containment barriers that are designed to safeguard lab workers, products, and the environment against biological agents. Field certification/verification of BSC operations is required at the time of installation and annually.

Recertification of Class II BSC is required whenever:

- a. HEPA or ULPA filter is replaced
- b. Maintenance of BSCs
- c. Internal repairs
- d. Cabinet is relocated

## High-efficiency Particulate Air Filters

HEPA filters have a minimum effectiveness of 99.99 percent in removing the most penetrating particle size, or MPPS, of approximately 0.3  $\mu\text{m}$ . They can effectively remove micro contaminants from BSC air and manage airborne particulate materials within it.



*Figure 13: HEPA filters*

# Section IX: Laboratory Waste Management

## Definition:

“A waste, or a mixture of wastes, which can cause or significantly contribute to an increase in morbidity and death due to its amount, concentration, or physical features.” A rise in serious, permanent, or incapacitating sickness poses a significant current or potential threat to human health and the environment. When handled, stored, transferred, disposed of, or otherwise managed inappropriately.

## Types of Biological Waste

- **Physical** – Disposed in biological bags  
Culture plates and tubes, loops, plastic ware, PPE, paper towels, animal carcasses, general hospital and laboratory waste
- **Liquid** – Disposed through sewer system  
Cultures, spent culture media, blood or other bodily fluids, byproduct of instrument/equipment decontamination
- **Sharps** – Disposed in labeled closable, puncture-resistant sharps containers  
Needles, scalpels, razor blades, broken glass, pipette tips, glass slides and coverslips

Various categories of waste in a laboratory:

1. **Hazardous** waste, which contains biohazards and is thought to be harmful to human health and the environment, is divided into several subcategories.
2. **Non-hazardous** or general waste is a type of waste that poses no physical or health risk to laboratory staff, the community, or the environment. This category covers waste created by the facility's administrative, housekeeping, packing, and maintenance tasks, and is classified as either general or municipal waste. Non-hazardous garbage should be deposited in a white waste bag-lined container.
  - This category of garbage is further separated into recyclable, non-recyclable, and biodegradable waste; color coding can be changed.

## Subcategories

1. **Infectious Waste** includes pathogens such as bacteria, viruses, parasites, or fungus, or is reasonably suspected of containing them, and creates a risk of disease transmission to humans or animals. Blood and other bodily fluids, or anything contaminated with them, microbiological cultures and stocks, carcasses of infected or potentially infected animals from laboratory facilities, all types of cell lines and cell cultures, diagnostic laboratory samples of human or animal origin, or anything in the laboratory, including PPE, that has been exposed to contaminated items or is suspected of being contaminated with pathogens, are all examples of infectious waste.

This garbage should be deposited in a sturdy rigid plastic container with a yellow waste bag inside. When not in use, the container should be close fitted with either a pedal type or plastic lid.

2. **Sharps Waste** is a form of biomedical waste composed of used "sharps," which includes any device or object used to puncture or lacerate the skin
  - Should always be considered contagious, whether used or clean
  - In a perfect world, needles would not be cut at the time of use and would be discarded into a yellow sharp receptacle
  - With the syringe in place, a needle is considered sharp
  - A sharps container with a tight aperture and a cover should be puncture resistant and leak proof

- Sharps containers should be labeled the same as other infectious/risk waste containers, but with the addition of a "DANGER! SHARPS" indication
  - Three-quarters-filled sharps containers can be filled with bleach. Cover the contents with 5 percent bleach to disinfect the sharps and then place them in a yellow waste bag with the lid properly closed or sealed, if the final treatment of the yellow waste bag is incineration in the laboratory
3. **Potentially Infectious Pathological/Anatomical Waste** includes human/animal body parts, organs, tissues, leftover blood or blood products, and fetal material.
- This garbage is deposited in yellow waste bags and labeled the same as other laboratory waste
  - Recognizable body pieces or a fetus can be separated from the infected waste stream, tagged, and packed for allowed burial, depending on religious or cultural preferences
  - Also, if adequate proof exists that any waste item in this category is not contagious, it can be classified as non-hazardous waste

## Processes of Waste Management

The processes for waste management include the following.

1. Minimization
2. Segregation
3. Packaging
4. Labeling
5. Collection
6. Storage
7. Transport

### Minimization

Both hazardous and non-contaminated trash should have a waste reduction, reuse, and recycling program implemented as part of the waste management strategy and plan. Waste reduction is the most preferred waste management strategy since it delivers remedies at the source rather than at the end of the pipe. A waste minimization program should consider the following:

1. **Managing inventory and stock:** Laboratory inventories should be effectively managed to minimize waste, such as outdated sera, blood products, reagents, chemicals, and medications. The goods' expiration dates should be compared to their per-day or per-week consumption at the time of purchase. Items that may expire before their intended use should not be purchased and should instead be managed on a first-come, first-served basis.
2. **Selecting products:** Products with the fewest package layers and no additional components or accessories should be preferred. When purchased individually, several of the components can be used with a variety of different kits for similar or related purposes, reducing waste.
3. **Choosing a supplier:** In an organization's waste minimization plan, suppliers are vital stakeholders and accountable partners. Suppliers who can provide modest amounts of items quickly and on schedule should be favored. They should also accept unopened items for return.
4. **Selecting a method:** Cleaning, disinfecting, testing, and documenting methods that create less waste should be implemented. Physical cleaning and disinfection measures, for example, should be favored over chemical approaches. In some circumstances, electronic documentation may be preferable to paper documentation

### Segregation

1. Segregation refers to the classification of all waste generated in an institution, such as a hospital, into distinct waste classes based on treatment and disposal needs.

2. The person creating the waste is responsible for separating non-risk and risk waste at the point of generation.
3. Segregation should be done as near to the work area as feasible, which means using a distinct set of trash containers for each bench, biosafety cabinet, and small room.
4. A common rule is to keep dumpsters at arm's reach and at a reasonable height for those working in laboratories. Spills, exposures, and injuries will be reduced as a result.
5. Different forms of garbage should be separated into colored containers. If solid waste containers from a certain waste category, such as infectious waste containers, are re-used in the laboratory, they should be lined with the same-colored waste bag.
6. Different color-coding systems can be used in different laboratories if everyone in the lab and the waste handlers are aware of them.
7. Due to inaccurate visual identification of the waste bags, the danger of unintentional mishandling at the treatment site increases.

## Labeling

1. A garbage container or bag should be tagged so that it may be tracked back to its source if needed.
2. Tagging will enable waste handlers to track issues with waste segregation and obtain critical waste information in the event of an accident.
3. Waste containers or bags should be labeled with an international hazard symbol, the kind of waste, the date of packaging, the department and laboratory/facility name, contact information, and the initials of the person who packed the bag.
4. Where possible or necessary, weight can be stated on trash containers/bags.
5. For a laboratory, a simple labeling strategy is to create a customized and standardized label for its trash that can be easily pasted on the waste bag/container.
6. These types of labels will help in receipt of complete and uniform information.



Figure 14: An example of a label for infectious waste

The international hazard symbols are shown in the figure below.

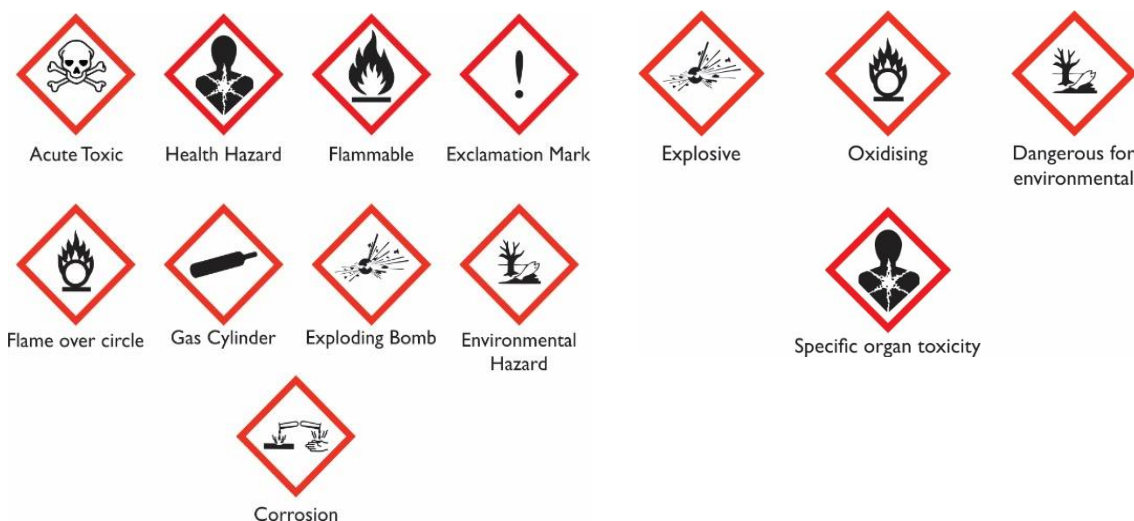


Figure 15: International hazard symbols

## **Pharmaceutical Waste**

These include heavy metal containing medications, restricted drugs, and antibiotics. Generally, brown cardboard boxes are used for this sort of garbage, with the name of the major waste item and any relevant danger label, as well as any labeling specifications indicated in the labeling section. Substantial amounts of pharmaceuticals can be returned to their suppliers, who will return them to the production plant or to specialized waste treatment facilities in their original packaging.

## **Waste Containing Radioactivity**

Biological laboratories frequently generate low-level radioactive waste, which, despite its modest quantity, should be treated with utmost caution. It should be packed in yellow leak-proof heavy-duty plastic bags made of polyethylene, polyurethane, or polyvinyl chloride for radioactive waste. With a few exceptions, different radioactive isotopes should be stored in separate lead-lined containers or bags.

In addition to other labeling characteristics, the waste bags should be tagged with the radiation symbol, name, and activity of the radionuclide on a certain date, as well as the required storage term. Based on its infectious or non-infectious hazard characteristics, this radioactive waste should be placed in normal yellow or white bags after decaying to background levels. For high-level and relatively long-half-life radionuclides, the supplier's packing and storage instructions should be followed under the supervision of a radiological officer, and then returned to the supplier for final disposal.

## **Chemical Waste**

This includes waste polluted with heavy metals, such as mercury and cadmium, as well as wasted chemicals created during disinfection treatments, cleaning processes, laboratory reagents, and solvents used in diagnostic and experimental activities. Chemical waste should be collected in color-coded, leak-proof, chemical-resistant containers that are labeled with the primary chemical's name and related danger symbols such as poisonous, corrosive, flammable, reactive, explosive, and shock sensitive.

If the laboratory expects to produce multi-hazardous waste, it should make sure that the waste management strategy includes segregation, labeling, packing, and storage methods for this sort of waste. The sequencing and methods of treatment for distinct dangers determine the segregation of this type of waste, which should be labeled and packed properly. Staff who perform segregation should receive regular and refresher training. This will considerably eliminate concerns with segregation and promote adherence to SOPs.

## **Collection and Packaging**

To eliminate spills and leaks during storage and transit, a waste bag should be carefully packed using self-locking plastic sealing tags, a simple knot, or the goose neck method. Once closed, the trash bag should never be opened again. After packing, disinfectant should be rubbed down the outside of the trash bag or container.

It is critical to establish and finalize a trash collection strategy in conjunction with the appropriate garbage collection authorities. A waste management strategy should include garbage pickup schedules. During tea and lunch breaks, as well as the laboratory staff's duty off/on schedules, the collection should be prevented. The waste transportation routes chosen are documented in the waste management plan for waste delivery from the laboratory to a central storage facility. If a trash bag/container is three-quarters full before the scheduled collection time, it should be packed and replaced promptly.



Table 5: List best practices for collecting waste from different laboratory sections or departments

<b>Best practices for collecting waste</b>
<b>Separation of waste collection equipment (trolleys, etc.) for risk and non-risk waste</b>
<b>Development of a waste collection plan in consultation with the waste collection staff</b>
<b>Regular collection on fixed timings and at least once a day</b>
<b>Availability of sufficient staff for waste collection</b>
<b>Separate collection timings for risk and non-risk waste</b>
<b>Uninterrupted supply of waste bags/containers, PPE, and waste collection equipment, such as trollies</b>
<b>Immediate placement of a new waste bag into the waste container after collection of filled bag and immediate replacement of filled containers with new containers</b>
<b>Thorough cleaning of waste containers in between the replacement of waste bags</b>
<b>Supervision of the waste collection staff to monitor adherence to the best waste collection practices</b>
<b>Development of a contingency plan in case of an event delaying waste collection</b>
<b>Documentation of the quantities of the waste generated daily or weekly, when possible</b>

## Storage

The waste created by laboratories can be held in an interim/short-term storage area, where it is temporarily stored after collection, or in a central storage area, where it is stored until it is collected for offsite transport and/or final treatment and disposal.

In both circumstances, it should be a secure enclosed facility with limited access away from food preparation and storage areas. Supply should be sufficient of face masks, workplace aprons, industry boots, and disposable or heavy-duty gloves (as necessary), waste bags/containers, spill kit, and cleaning equipment near an on-site treatment facility, such as an incinerator. Cleaning a trash storage space at least once a week is recommended. Waste should not be kept in the central storage facility for longer than 24 hours and should be stored at 3–8°C.

## Transport

A container of appropriate size for the vehicle's layout, a suitable technique for securing the cargo during transport, emergency equipment such as a spill kit, and an easily cleanable vehicle interior surface are needed. On the vehicle, the garbage carrier's name and address, an international hazard notice, and an emergency phone number should be provided. Details about the garbage should be given to the driver.

## Decontamination Methods

Several methods have been successful in treating infectious waste:

- a) Autoclaving (steam sterilization)
- b) Incineration
- c) Thermal inactivation
- d) Gas/vapor sterilization
- e) Chemical disinfection
- f) Sterilization by irradiation (radiofrequency and microwave)

## Physical Waste Management

### Incineration:

**Onsite:** seal bag, disinfect outside with suitable disinfectant, store, and carry to incinerator.

**Offsite:** seal bag, disinfect exterior with appropriate disinfectant, store in a secure location, and track transport to the incinerator.

### Autoclave:

**Onsite,** loosely close the bag, treat the outside with the necessary disinfectant, transport to the autoclave, and check the autoclave cycle.

**Offsite:** wrap bag loosely, disinfect outdoors with suitable disinfectant, store in a secure area, and track transfer to the autoclave. Detailed SOPs are provided in Annex 12.

### Dump:

Chemically treat all physical waste before dumping in the landfill by ensuring that it is exposed to a suitable disinfectant for the requisite contact period. All biological waste should be treated in accordance with municipal and organizational policies.

## Liquid Waste Management

All liquid waste **MUST** be chemically treated<sup>5</sup> before being poured down the sewer

## Sharps Waste Management

Sharps should be kept in a puncture-resistant container, which should be disinfected on the outside before being stored and transported to an incinerator. Keep sharps in a puncture-resistant container, treat inside sharps container with suitable disinfectant, wipe off exterior of sharps container with appropriate disinfectant, store and transfer to autoclave.

Chemically treat all sharps by ensuring that they are exposed to an adequate disinfectant for the requisite contact period. Grind stuff and make sure they are disposed of in a way that won't affect others' skin. Ensure that the plastic container may be autoclaved. Some polymers, such as polyethylene and HDPE, are not autoclaved.

## Reuse

Reusable goods should be promoted for use in laboratories if they do not impair job quality or the safety of the environment or employees. The use of disposable products in a laboratory with a faulty waste management system can put the environment and people at greater danger than using reusable items by increasing waste volumes.

Similarly, because of the significant danger involved with high-risk infections and procedures, reuse is not advised in maximum containment laboratories. Before being handled as non-infectious materials, reusable items must be decontaminated and cleaned. Items that will be reused in an organization should be documented in the waste management strategy, and written processes for separate collection and subsequent processing should be in place.

## Recycling

Recycling is less desirable in a laboratory than minimization and reuse, since it requires more effort on the waste products, including transportation to an offsite recycling facility. Environmentally preferred purchasing, which includes items that are less harmful to the environment and are reusable or recyclable, should be encouraged.

---

<sup>5</sup> <https://www.epa.gov/coronavirus/disinfectant-use-and-coronavirus-covid-19-list-n-disinfectants-covid-19.pdf>

# Section X: Transport of Infectious/Biological Materials

The USAID-donated mobile biosafety level 2 labs are equipped for diagnosing priority infectious diseases, primarily for COVID-19, HIV/AIDS, and tuberculosis.

## Definitions

A pathogen or biological agent that may cause disease in people or animals, such as bacteria, viruses, parasites, rickettsia, fungus, or other agents, is known to be present in an infectious substance. Prions, for example, are proteinaceous infectious particles.

Infectious substances are divided into three categories:

1. Infectious Substances Category A
2. Biological Substances Category B
3. Exempt Substances

## Category A (Infectious Substances)

- These are characterized as substances that might induce an infectious illness in otherwise healthy individuals or animals when exposed during transportation, resulting in lifelong impairment or death
- Category A infectious substances that match these requirements and can cause disease in people or both humans and animals have been given the UN identifying number "UN 2814"
- Category A infectious substances that match these requirements but can cause only sickness in animals have been assigned the United Nations identification number "UN 2900"

## Category B (Biological Substances)

- Category B is defined as infectious material that does not meet the criteria for inclusion in Category A
- Category B has been allocated UN 3373 "Biological Substance"

## Exempt Substances

- A sample that is free of infectious substances or that contains compounds that are unlikely to cause disease in animals or people
- Substances that are free of infectious substances or are unlikely to cause disease in people or animals
- Microbes that are incapable of causing infection in people or animals
- Pathogens that have been deactivated, disabled, or neutralized so that they no longer pose a hazard to human and animal health
- Environmental samples (such as water and food) that do not provide a major risk of infection in humans and animals
- Transfusion-related blood or blood components
- Fecal occult blood screening samples and dried blood stains
- Patient specimens with a minimal risk of infections—labeled "exempt human specimen" or "exempt animal specimen" on the packaging
- Decontaminated health care or laboratory waste

Types of specimens requested for transport or transfer by air, rail, road, or ship include the following:

1. **Pathogen cultures:** Intentionally generated pathogen cultures. Patient specimens are not included.
2. **Patient specimens:** These are samples taken from people or animals for study, diagnostic evaluation, investigations, treatment, and prophylaxis. Secretions, blood, serum, plasma, excreta, cellular parts, tissues, and tissue fluid swabs taken from any part of the body.

3. **Biological products:** These products are derived from living organisms and are primarily used for disease prevention, treatment, or diagnosis in humans and animals, as well as research and development. They also include vaccines, either complete or incomplete.
4. **Genetically modified organisms (GMOs):** Organisms whose chromosomes have been manipulated or changed by genetic engineering. The shipment is like that of other infectious agents. GMOs that do not meet the requirements for infectious substances are given the UN 3245 identification number.

**Triple packaging:** To safeguard the contents being carried, triple packing offers three levels of control and confinement: primary, secondary, and tertiary.

## Category A Packaging

The package contains:

- a. A watertight container
- b. A watertight secondary receptacle (to contain any spilled liquid materials)
- c. An absorbent substance within the secondary receptacle capable of absorbing any sample leak in the primary container (capable of protecting the contents)

The following performance tests must be passed by the entire packet's structure:

- a. Leak-proof primary container
- b. Leak-proof secondary container
- c. Rigid outer container
- d. Pressure-bearing capacity of 95 kPa
- e. Drop test from a height of 9 m
- f. Puncture resistant at 7 kg pressure

In addition to these requirements, the package is also required to have:

- a. A UN identification code
- b. A certified/trained technician who prepares the contents for shipping
- c. Proper shipping documents, including emergency response information

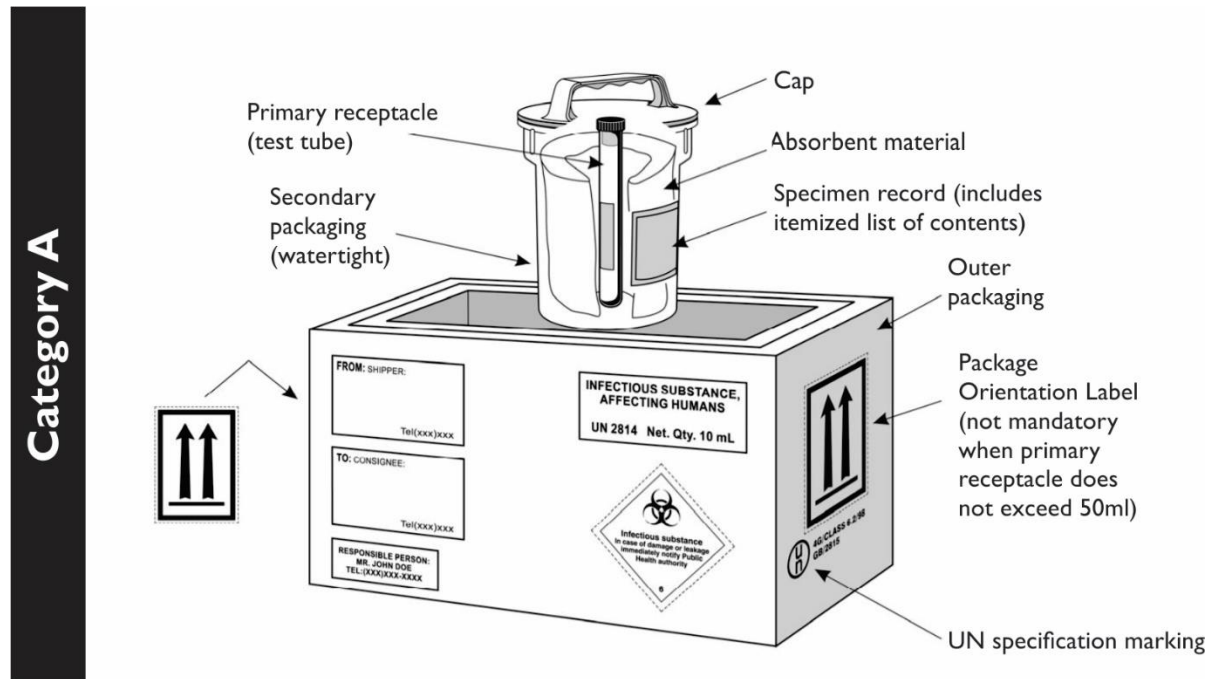


Figure 16: Example of a triple packaging system for the packaging and labelling of Category A infectious substance  
(Source: LATA, Montreal, Canada)

## Category B Packaging

Before packaging for shipping or transit, it is critical that this category meet the following requirements:

- Primary container is leak proof
- Secondary container is leak proof
- Pressure tested at 95kPa
- Either the secondary or outer container is stiff
- Drop tested from 1.2 meters

If traveling by air, the following conditions must be met:

- Minimum outer-container dimension of 100 mm (4 inches)
- Able to withstand shocks and loadings during transportation
- Able to absorb vibrations, changes in temperature, and humidity in addition to pressure
- Secondary package must contain enough absorbent material
- Accompanied by all required information, including the name of the responsible person/institution, address, and telephone number

The receptacle for these types of samples must have the following properties for transport:

- Primary container is leak proof
- Secondary container is leak proof
- Outer packing with adequate strength

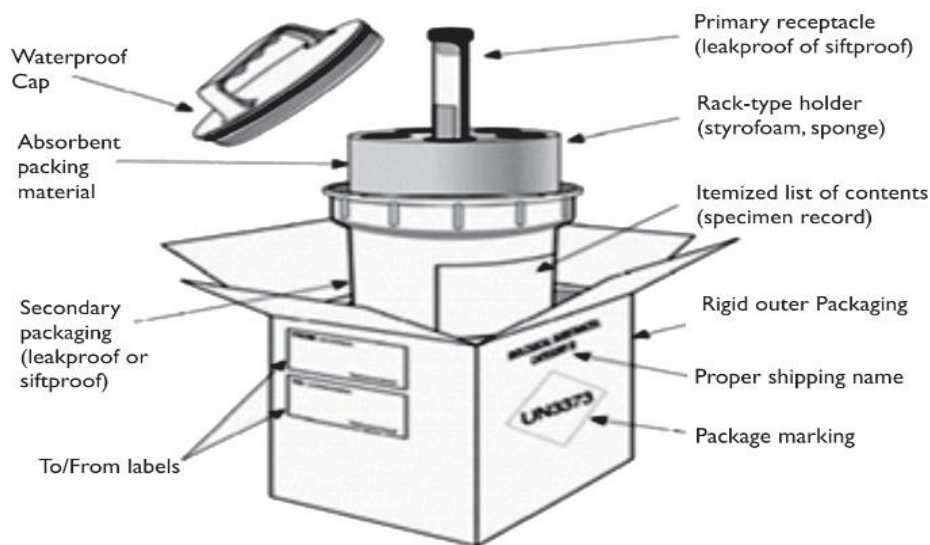


Figure 17: Standard triple packet system as per WHO classification for packaging and labelling Category B (Source: LATA, Montreal, Canada)

## Steps for Packaging Samples

- Form the outside receptacle
- Insert the inner lining
- Remove the secondary receptacle's lid
- Place an equivalent material for spill absorption
- Put on disposable gloves
- Wrap cushion material around the primary tube
- Place the main container into the secondary container
- Remove disposable gloves

- i. Secure and close the secondary container
- j. Place the secondary container into the inner lining (and outer container)
- k. Place the laboratory test instructions inside secondary container
- l. Close and pack the secondary container
- m. Ensure that the labeling and marking of Category A packages have been completed

## Sample Transfers

Any pathogen movement between a mobile laboratory and an institution that requires use of a motor vehicle on public roadways must meet these requirements. However, if pathogen mobility is restricted to the bounds of a mobile laboratory and the institution where they are stationed, and is not commercial transportation, these regulations do not apply.

If the main container spills, the sample is placed in a sealable bag or container to create a leak-proof primary container with absorbent material in the container or bag. For transportation, the absorbent primary container with absorbent material is put in a sturdy, rigid outer container, or receptacle. During the sample transfer, the exterior surface of the receptacle must be disinfected, and PPE must be worn according to the risk assessment.

## Shipping in Pakistan

Local courier services have begun to adhere to international and national regulations. From the time the package is shipped, all steps in the shipping of such materials must be recorded, and the package must be tracked through written documents. The shipment's generator retains ownership.

For the shipment of Category A drugs, training in infectious agent shipment is required, and this training should be delivered on an institutional basis. Laboratory managers, pathologists, microbiologists, technologists, technicians, and phlebotomists are among the target audience for these trainings, which are being organized by the NIH and the PBSA. TCS, M&P and Leopards couriers are already involved in sample transport from the field to NIH and DHL, mostly for international shipments.

# Section XI: Biological Emergency Response Procedures and Incident Reporting

Every laboratory should have an Emergency Response Guide. Spill protocols, exposure procedures, incident procedures, reporting instructions, contact numbers, and emergency equipment locations are all included in the manual. The laboratory supervisor or a designated lab safety coordinator must review the advice with fresh staff.

All injuries, accidents, animal bites, and exposures should be reported to your provincial lab focal person, and the Incident Report Form should be completed (format provided).

## Biological Materials Exposure

1. Remove contaminated clothing, shoes, jewelry, etc.
2. Immediately flood exposed areas with lukewarm water from a safety shower, eyewash, or faucet for at least 15 minutes (use soap on skin for biological/blood exposure). Hold eyes open to ensure effective rinsing behind both eyelids.

## Needlestick or Cut with Contaminated Sharp Item

Few emergency response situations require immediate action. However, if someone experiences a needle-stick injury, the amount of time taken between the actual incident and dilution of the exposure could increase the risk of illness. Remember that an exposure does not always cause illness, and by minimizing your exposure, you may minimize the likelihood of illness.

- a) Needle Stick Injury
- b) Red, Yellow, and Green Evacuation
- c) Spill Management (Major and Minor)

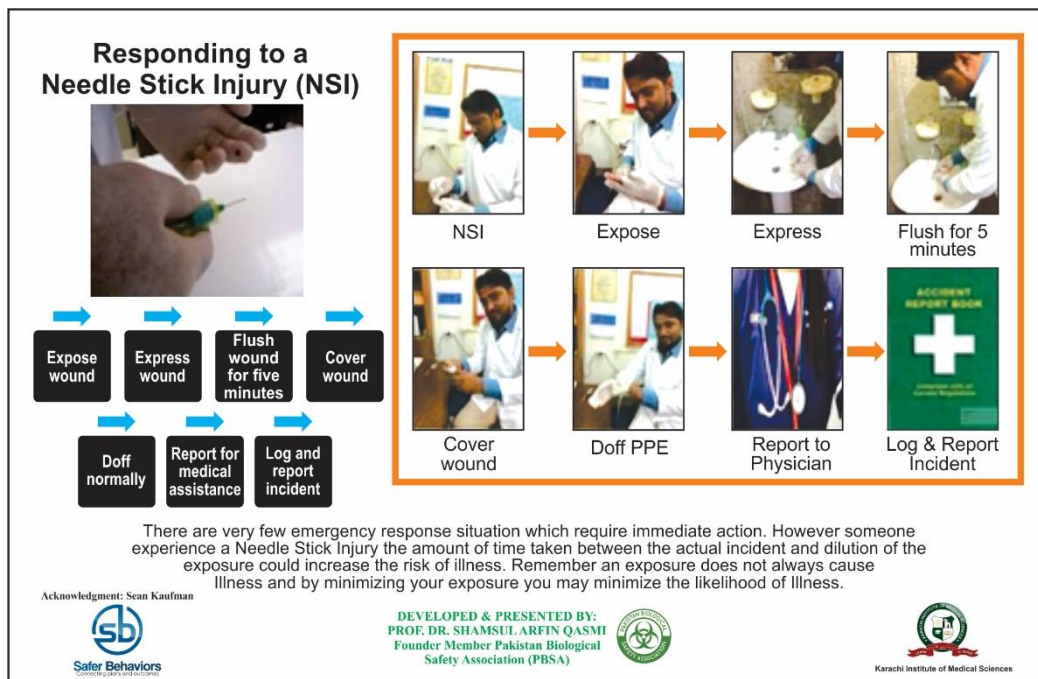


Figure 18: Needle stick Inquiry



## Emergency Evacuation

Laboratory staff should be prepared to respond to any emergency and be able to demonstrate these processes of evacuation.

These can be classified as:

1. Normal Evacuation
2. Modified Evacuation
3. Rapid Evacuation

### Normal Evacuation (Green)

When a fire or critical support system alarm occurs, green evacuation takes place immediately. Call for further information, don't panic, advise patients, safeguard their work (samples/pathogens), evacuate the institution using standard decontamination procedures, and document and report the occurrence. Fire safety protocols are covered under Fire SOPs in Annex 13.

### Modified Evacuation (Yellow)

When a staff member is unconscious or injured, the ability of the rest of the crew to follow regular evacuation protocols is compromised. Staff at the facility are being instructed to leave immediately using modified decontamination procedures.

Containment is kept by modifying evacuation procedures.



Figure 19: Yellow Evacuation

Health Safety and Environment (HSE) drills are followed by other employees and patients.



## Rapid Evacuation (Red)

When life is in danger, red evacuation happens promptly. Along with the patients, facility workers are instructed to vacate the area as soon as possible using whatever means are available. Containment was not maintained, and a significant danger of fatality existed.

## Spill Management

For cleaning spills, several institutions have different SOPs. Regardless, any SOP for cleaning a laboratory spill should include the following (outside a BSC):

1. Inform everyone in the laboratory that there has been a spill
2. Change PPE
3. Clean the spill from outside in
4. Allow enough contact time
5. Always document and report spill events

Steps for proper spill workup:

1. Notify co-workers right away (proximity)
2. If you're wearing gloves or boots, take them off and put on fresh PPE
3. Obtain a spill kit
4. Display spill signs
5. Determine the spill parameter
6. Soak towels in your disinfectant of choice
7. Cover spills with towels while working outside-in
8. Remove the boots and gloves and put on fresh PPE
9. Allow enough time for interaction
10. Pick up towels when working outside
11. Use biohazard bags to dispose of towels and garbage
12. Clean up spills
13. Don fresh PPE and remove boots and gloves
14. Keep track of and report incidents

Table 6: Spill kit requirements

Items required	Quantity required for one kit
Disposable gowns	1
Gloves (double if necessary)	1 box
Disposable shoe covers	1 set
Head caps	1
N-95 respirator	1
Mask	1
Goggles or full-face shield	1
Absorbent paper towels	3–4 sheets
Spill pillows for large spills	2
Small disposable dustpan and brush	1
Tongs or forceps for sharps	1
Biohazard waste bags	2–3
pH indicator strip	1
Neutralizer for acidic spill	1
A waterproof copy of SOP spill response and cleanup procedures	1
One large plastic box	1

## Spill Inside the Biosafety Cabinet

A spill or release contained within a BSC poses no risk to those in the lab or the environment because the BSC's purpose is to confine the spill and protect lab staff from exposure. Decontaminate everything inside the BSC, including the operator's hands and arms, any equipment in the BSC, and the BSC's interior surfaces. Clean-up will be easier if the BSC's work surface has been lined with absorbent material.

Simply roll up the liner so that the contaminated area is on the inside and dispose of it properly to a biohazard container. Seal the bag.

Or else:

- Keep the BSC switched on
- Have someone else in the lab to prevent contamination outside of the BSC
- Carry a biohazard trash container and new PPE
- If wearing infected gloves or sleeve coverings, remove them and place them in the hazardous waste box
- Put on new PPE before returning arms and hands to the cabinet
- Before removing reusable items from the BSC, disinfect them with a chemical disinfectant
- Place all discarded items in the biohazard waste container
- Place all sharps in a sharp container and dispose of them properly
- Clean the BSC's cabinet walls, work surfaces, and equipment with a certified disinfectant

SOPs for rapid inactivation are provided in Annex 15.

## Spill, Release or Aerosolization Inside a Centrifuge

To begin,

- Do not inhale; close the centrifuge lid
- Notify others that they should exit the lab

Afterwards

- Leave the lab right away
- Place biohazard spill warnings outside lab doors
- Re-enter the laboratory after 30 minutes to allow the aerosol to settle before cleaning up
- Remove PPE and disinfect on a spot basis where possible
- Wash any exposed parts with antiseptic soap and warm water
- Wash hands thoroughly

# Section XII: Decontamination and Disinfection of Laboratory

Laboratory-associated infections (LAIs) are disseminated to laboratory workers directly or indirectly through contaminated sources such as air, fomites, lab equipment, splashes, and aerosols. Cleaning and surface disinfection or sterilization methods are commonly used in laboratories to decrease the risk of infection spread.

Also, thorough handwashing and the use of PPEs are critical in safeguarding laboratory employees.

A laboratory biosafety program is implemented using the following methods:

1. Cleaning
2. Disinfection
3. Sterilization
4. Decontamination

## Cleaning

Cleaning involves the physical removal of bacteria and other related pollutants (e.g., blood, tissues, culture media) from a surface to the amount required for subsequent processing. It may or may not have antibiotic action. Cleaning is a necessary step before disinfection or sterilization to ensure that disinfectants or sterilization procedures work properly. Furthermore, most biofilms need manual cleaning.

## Disinfection

Disinfection kills almost all known pathogens, but not all microbial forms found on inanimate surfaces, such as bacterial spores.

Many factors influence the efficacy of disinfection, including:

1. Types of organisms and their numbers (especially the bacterial spores)
2. The presence of organic materials (e.g., blood, feces, soil)
3. Types and condition of surfaces, instruments, and devices
4. Contact time
5. Temperature

## Sterilization

Sterilization is used to sterilize media, glassware, trash, and other materials. When an object, instrument, or solution is fully devoid of all live microorganisms, including spores and viruses, it is said to be sterile. Through this technique, a microorganism's chance of surviving on a treated object is less than one in a million, indicated by a sterility assurance level of  $10^{-6}$ .

## Decontamination

Decontamination makes a space, gadget, object, or substance safe to handle while also almost eliminating the potential of disease transmission. Decontamination in a laboratory context may entail cleaning an instrument, equipment, or space using soap and water. Sterilization processes such as steam autoclaving are often used for controlled lab waste, used lab materials, and laboratory articles.

Long autoclave cycles, incineration, or gaseous treatment of space and surfaces will be used to decontaminate spills, equipment, BSCs, or biological waste if highly hazardous pathogens are present in laboratory settings. Resistance of selected organisms to decontamination in descending order is presented in the figure below.

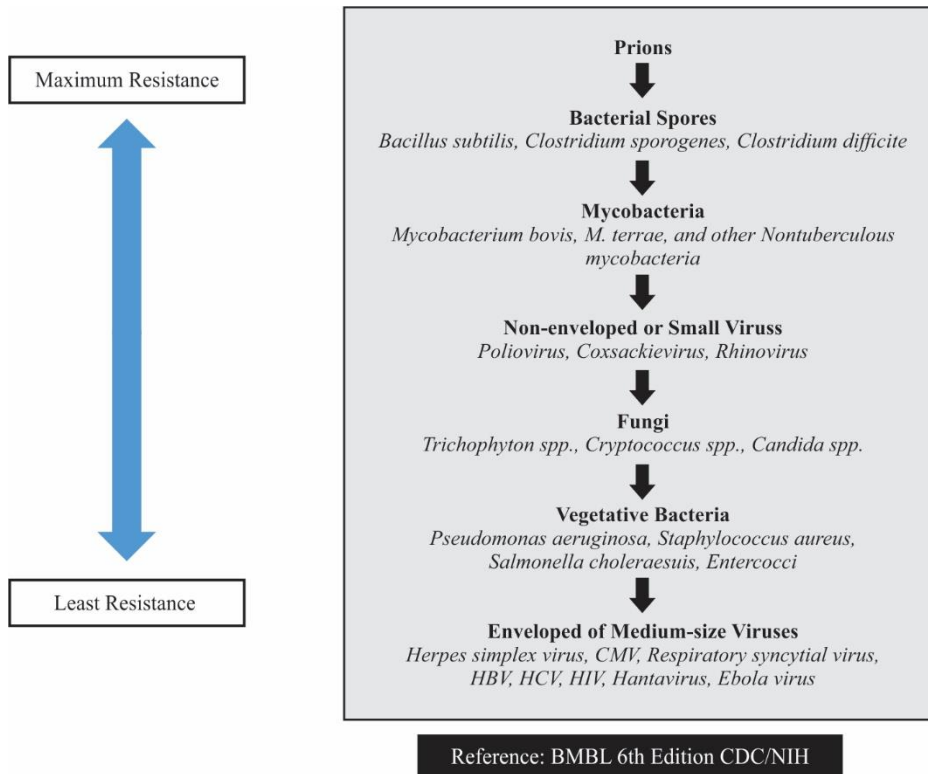


Figure 20: Descending order of relative resistance to disinfectant chemicals

## Section XIII: Biosecurity

The ideas and practice of biosecurity are used to prevent the intentional abuse or exposure of microorganisms and toxins to humans and the environment. Pathogens and toxins have been used to terrorize and damage individuals, to cause social disruption, and to destroy economies. Even though several international regulations and recommendations ban the use of biological weapons and the malicious use of germs, diseases have still been used as weapons of terror.

Following the anthrax attack in 2001, the world community became concerned enough to treat laboratory biosecurity as a serious international concern. Biosecurity must be implemented in laboratories by laboratory employees and management; however, it is not often taken as seriously as biosafety. In the laboratory, biosecurity necessitates a twofold obligation for personnel: securing biological material so that it cannot hurt others if accidentally exposed, or a guarantee not to use the items to intentionally harm others and preventing others from doing so.

The WHO's Laboratory Biosecurity Guidance (WHO, 2006) establishes a comprehensive biosecurity technique for laboratories. It emphasizes that laboratory personnel have an ethical, moral, and technical responsibility to safeguard the public and to demonstrate that biological hazards, which are inherent to laboratory work, are maintained with appropriate precautions for a safe global ecosystem.

Laboratory employees are required to operate responsibly and take steps to safeguard the community by not exposing themselves or others to bio risks. Laboratory staff must observe safe working procedures, keep samples safe from purposeful release or theft for malevolent purposes, and adhere to a bioethics and biosecurity code of conduct. While the work of these institutions serves people all over the world, dealing with infectious organisms and their products presents hazards that must be regularly monitored.

### Risk Assessment

The chance of a pathogenic (biological) agent being taken (theft) from a secure environment and the repercussions of an epidemic after a deliberate release of that agent are both considered in biosecurity risk assessment. In other terms, biosecurity risk equals (threat potential) x (consequences). Biosecurity has five components:

1. Physical security
2. Personal security
3. Inventory and material control
4. Information protection
5. Transportation safety

Biosecurity has just gained three additional elements: (WHO Biosafety Manual 4th Edition)

1. Incident/emergency response plan
2. Emerging biotechnology
3. Dual Use Research of Concern

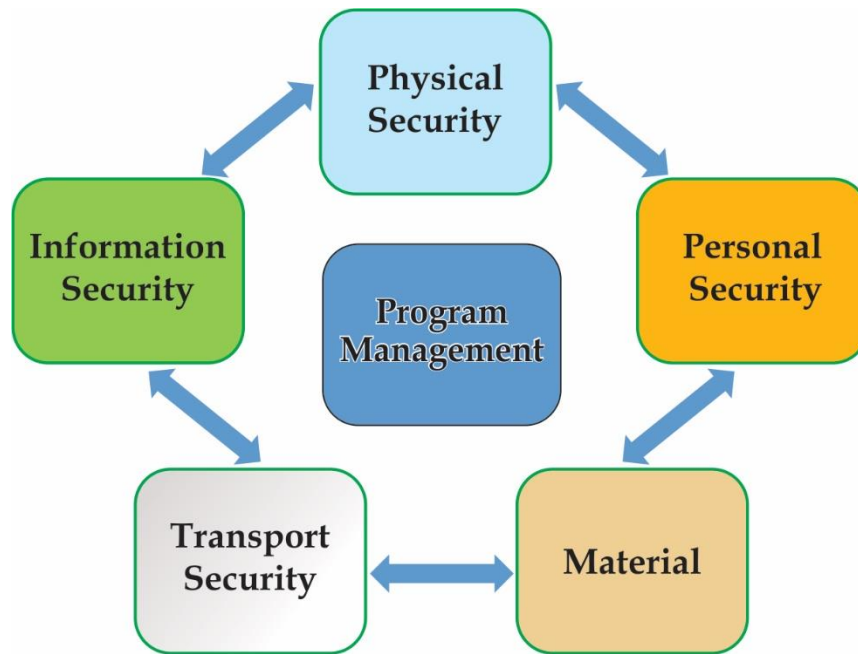


Figure 21: Elements of Biosecurity

## Physical Protection

Physical protection methods restrict access to areas of the facility that store biological agents and equipment. Perimeters and borders, access restrictions, and alarms/observations are examples.

## Personnel Security

Personal security measures are steps that have been implemented to reduce the risk of insider threats. Employee screening, categorization, employee ID cards, and guest escort regulations are some examples.

## Inventory Control

Measures were put in place to detect positive or negative disparities in biological inventory. Examples of these are:

1. Inventory (what, why, and how much)
2. Control (where)
3. Accountability (who, when, for what)

## Information Security

Procedures have been put in place to limit access to sensitive data and electronic controls. Passwords, firewalls, regulations limiting USB use, and policies governing information systems (e.g., email, servers, internet access/downloads, software installation) are some examples.

## Transport Security

Procedures designed to reduce the risk of insider and outsider threat during transit. Transport security serves as a control system to reduce the danger of theft from inside and outside as well as theft while biological substances are transferred between regulated and unregulated zones. Biological materials can be transported inside a facility, between facilities, within a country, and between continents. Internal and external transportation policies are examples of this.

## Emerging Biotechnology

Emerging biotechnology encompasses genetically engineered microbes, synthetic biology, stem cell research gain of function, gene editing, CRISPR, and gene drives. These advancements have been connected to better human, plant, and animal health.

Global health security, economic prosperity, informed policymaking, and public trust and faith in science are all improved through life sciences research. However, accidents and their possible willful abuse pose hazards, necessitating adequate management methods to mitigate these risks and proceed with valuable life sciences research.

## Dual-Use Research of Concern

Life sciences research of concern is research that, based on current understanding, has the potential to generate knowledge, information, products, or technology that might be directly misapplied to pose a major hazard to:

- Public health and safety
- Other plants
- Animals
- The environment
- Agricultural species

Where relevant, awareness of the dual use of agents, equipment, and technology should be factored into the establishment of laboratory biosecurity strategies. Laboratories should accept responsibility for the dual-use nature of such agents and experiments, such as genetic editing, and follow national rules when deciding on biosecurity measures to prevent unauthorized access, loss, theft, misuse, diversion, or purposeful release. The potential for biosciences to be misused is a worldwide problem that calls for a balanced approach to laboratory biosecurity to provide lawful access to critical research and therapeutic materials.





## References

1. Biosafety in Microbiological & Biomedical Laboratories 6<sup>th</sup> edition, BMBL 6<sup>th</sup> Edition CDC NIH <https://www.cdc.gov/laboratories/BMBL.html>
2. CEN Workshop agreement CWA 15793-2012 <https://internationalbiosafety.org/wp-content/uploads/2019/08/CWA-15793-English.pdf>
3. Division 6.2 Infectious Substance Shipping Guide: Classification, Packing, Marking and Labeling. Massachusetts Department of Public Health. William, A.H. State Laboratory Institute 2012. <https://www.mass.gov/doc/division-62-infectious-substance-shipping-guide-classification-packing-marking-and-labeling/download>
4. Good Clinical Laboratory Practices in Pakistan 2019 <https://www.nih.org.pk/wp-content/uploads/2019/04/HANDBOOK-for-Good-Clinical-Lab.pdf>
5. Guidelines for the Safe Transport of Infectious Substances and Diagnostic Specimens. WHO Division of Emerging and Other Communicable Diseases Surveillance and Control 1997. <https://apps.who.int/iris/handle/10665/63564>
6. Harvard Biosafety Manual 2016 [https://www.ehs.harvard.edu/sites/default/files/biosafety\\_manual\\_0.pdf](https://www.ehs.harvard.edu/sites/default/files/biosafety_manual_0.pdf)  
<https://blog.ansi.org/ansi-49-2020-biosafety-cabinets-bscs/#gref>  
[https://epd.punjab.gov.pk/system/files/Punjab%20Hospital%20Waste%20Management%20Rules%2C%202014\\_0.pdf](https://epd.punjab.gov.pk/system/files/Punjab%20Hospital%20Waste%20Management%20Rules%2C%202014_0.pdf)  
<https://nap.nationalacademies.org/catalog/4911/prudent-practices-in-the-laboratory-handling-and-disposal-of-chemicals>
7. Infectious Substances Shipping Guidelines 58th Ed. IATA Dangerous Goods Regulations 2017. [https://www.labelmaster.com/shop/iata?gclid=CjwKCAjw682TBhATEiwA9crI39A445I5O3j8ecqyVOYiu\\_foxGgBjTndjdvYA35gO3MJ9HaewQMzKBoCXt0QAvD\\_BwE](https://www.labelmaster.com/shop/iata?gclid=CjwKCAjw682TBhATEiwA9crI39A445I5O3j8ecqyVOYiu_foxGgBjTndjdvYA35gO3MJ9HaewQMzKBoCXt0QAvD_BwE)
8. ISO 35001:2019 Bio risk management for laboratories and other related organizations <https://www.iso.org/standard/71293.html>
9. Laboratory Biosecurity Hand book 2007 By Reynolds M. Salerno, Jennifer Gaudioso, Benjamin H. Brodsky <https://www.taylorfrancis.com/books/mono/10.1201/9781420006209/laboratory-biosecurity-handbook-reynolds-salerno-jennifer-gaudioso-benjamin-brodsky>
10. National Research Council, 1995. Prudent practices in the laboratory: handling and disposal of chemicals. National Academies Press.
11. NSF/ANSI Standard 49 2020
12. Punjab Hospital Waste Management Rules 2014
13. The Dangerous Goods Regulations of the ICAO Technical Instructions for the Safe Transport of Dangerous Goods by Air. ICAO Ed.: 2015-2016. <https://www.icao.int/safety/dangerousgoods/pages/technical-instructions.aspx>
14. WHO Bio risk management: laboratory biosecurity guidance 2006 <https://apps.who.int/iris/handle/10665/69390>
15. WHO Laboratory Biosafety Manual 4th Edition <https://www.who.int/publications/i/item/9789240011311>
16. WHO Safe Management of waste from healthcare activities. [https://www.euro.who.int/\\_\\_data/assets/pdf\\_file/0012/268779/Safe-management-of-wastes-from-health-care-activities-Eng.pdf](https://www.euro.who.int/__data/assets/pdf_file/0012/268779/Safe-management-of-wastes-from-health-care-activities-Eng.pdf)



## Annexes

- Annex 1: Security Management Plan
- Annex 2: Incident Management Plan
- Annex 3: Incident Reporting Form
- Annex 4: Serious Incident Reporting template
- Annex 5: Event Management I29
- Annex 6: Layout plan of the mobile BSL-2 laboratory
- Annex 7: SOPs for Avoiding Occupational Hazards Occupational Health Support Service Elements
- Annex 8: Rapid Inactivation Protocols
- Annex 9: Facility Security Plan
- Annex 10: Risk Assessment Tool
- Annex 11: Field Certification Protocols for Biosafety Cabinets NSF1/ANSI/49 Standard
- Annex 12: SOPS for Autoclave
- Annex 13: Fire Evacuation SOPs
- Annex 14: SOPs for Laundry
- Annex 15: Rapid Inactivation Protocols
- Annex 16: Technical Working Group for Mobile BSL-2 labs



## Annex I: Security Management Plan

# Mobile Bio Laboratory



## SECURITY MANAGEMENT PLAN

**Country**

**Location**

**MBL Tag No**

**Team Leader**

**Safety & Security Focal Person**

**Security Manager**

**Dated**

**Review Date**

**Custodian Name**

**Appointment**

A large, empty rectangular box with a light gray gradient background, intended for the completion of the security management plan details.

## Table of Contents

### Introduction

#### Section I – SECURITY MANAGEMENT

- 1.1 Establishing a Security and Incident Management Forum
- 1.2 Goals and Objectives
- 1.3 Structuring Teams
- 1.4 Accountability
- 1.5 Networking and Leveraging
- 1.6 Information Security
- 1.7 Risk Coding
- 1.8 Risk Rating
- 1.9 Crisis Management Decision Making
- 1.10 MBL Branding
- 1.11 Management Structures
- 1.12 Reports and Returns
- 1.13 Legal Requirements
- 1.14 Security Management Roles and Responsibilities

#### Section II – RISK MANAGEMENT

- 2.1 Risk Methodology
- 2.2 Risk Registry
- 2.3 Risk Assessments
- 2.4 Minimal Security Standards
- 2.5 Information Security
- 2.6 Incident Management and Crisis Response
- 2.7 Relocation of Critical Functions
- 2.8 Personal and Management Conduct

#### Section III – OPERATIONAL SECURITY

- 3.1 Security Controls
- 3.2 Travel Management
- 3.3 Location Security
- 3.4 Temporary Parking – Location Security
- 3.5 Investigations
- 3.6 Threats and Extortion
- 3.7 Pilfering and Theft
- 3.8 Communications
- 3.9 Medical Supplies
- 3.10 Recruitment and Vetting

#### Section IV – EMERGENCY PREPAREDNESS

- 4.1 Emergency Preparedness
- 4.2 Alert States
- 4.3 Trigger Response Plans
- 4.4 Alert Notifications
- 4.5 Incident Management Response
- 4.6 Crisis Response

#### Section V – TRAINING AND EDUCATION

- 5.1 Awareness, Training and Competency
- 5.2 Deployment Training
- 5.3 Specific Management Training Requirements

## INTRODUCTION

The Security Management Plan (SMP) is a collection of security policies, instructions, guidelines, protocols, procedures, systems, tools and systems designed to meet a wide spectrum of risks in a mobile biosafety laboratory (MBL). The SMP is designed to be used in its entirety as a holistic and integrated system by a security and safety focal person (SSFP) designated in each MBL. The plan has been designed to be applied in its entirety, or selected components can be used as appropriate for a particular region, depending on the nature and activities conducted by MBL, as well as the risk environment in which that MBL operates and the nature and composition of the assigned team.

**Responsibility:** *SSFPs are responsible for the day-to-day safety and security of their team. However, the facility security manager (deployed location) is responsible for providing security management support to protect personnel and assets. The GHSC-PSM Business Risk Department will provide technical guidance on security matters to facilitate lab security operations.*

This document is the overarching policy document that governs the approach to security and risk management. An additional document, the Incident Management Plan, is included to meet specific security and safety needs. This template will be personalized to include specific factors relevant to each operating region and requirements.

**Important Note:** *The plans have been written to provide education and instruction to meet the knowledge and experiences of an SSFP. The facility security manager will provide training and education to SSFPs and their respective teams to ensure smooth implementation of the plan. GHSC-PSM Business Risk Department will assist the facility security manager in developing security training modules and training of designated laboratory staff as per specific requests.*

The Security Management Plan is divided into sections and a series of annexes and supporting documents and tools so that elements can be used as needed. This structuring approach allows the plan to be broken into “bite-sized” chunks. Some are active and used often, and some are educational and referred to only when required. Others are foundational policy documents that provide strategic and operational guidelines. This approach also supports post-design adjustments and modifications with greater ease for SSFPs. Also, once developed, the plan is structured to enable ease of sustainment, with live and static data points:

- Live points: the elements that are personal to a location or region and that might change frequently. These points are captured in tables, charts, or diagrams.
- Static points: the elements that are universally applicable across multiple locations or regions and typically change infrequently. These points are captured within the main body of the text.

The Security Management Plan is designed to achieve multiple concurrent goals, to:

- Provide the governing ethos and principles of security and risk management
- Provide a logical structure to complex security requirements
- Provide education and awareness for non-security professionals
- Establish security standards and approaches
- Offer instructions and guidelines for the management of risk
- Ensure consistency in managing security services
- Provide effective tools, systems and methodologies for effective management
- Provide practical guidelines and instructions
- Integrate corporate and field activities more seamlessly

While abiding by the policies and procedures in this handbook always is important, no security plan can ensure protection against all possible threats. Common sense and judgment are key in making any security plan effective. Personnel need to follow basic precautions to help minimize individual and group risks when traveling to, or

operating within, remote or hostile areas of the country. The facility security manager (FSM) responsible for coordinating all MBL security and incident management is:

Name	Appointment	Email	Phone

The custodian of this specific plan for each MBL is:

Lab Identification No: \_\_\_\_\_

Name	Appointment	Email	Phone



## SECTION I

### SECURITY MANAGEMENT

#### I.1 Establishing a Security and Incident Management Forum

The FSM will take ownership of risk and security management functions, as well as incident and crisis management roles. A local incident management team (IMT) from the MBL deployed staff will be developed under this plan. Creating the basic structure first, with the most critical appointments, is recommended, before expanding the organization to a mature stage. Two fundamental stages are recommended:

1. Critical structure: Establishing the core security and incident management team with the critical appointments and role and responsibilities.
2. Mature structure: Fleshing out the security and incident management teams and creating more departmental and individual specificity to roles and responsibilities.

Understanding the distinction between “incident” and “crisis” management is essential:

1. Incident management: the team dealing with the practical requirements of a crisis, typically the MBL field team or those at the point of crisis (the IMT)
2. Crisis management: the team dealing with the strategic and supporting functions of a crisis; facility security manager; the crisis management team has technical security guidance available from GHSC-PSM BRD.

#### I.2 Goals and Objectives

The goal of security management is to create conditions conducive to safe and productive work. The Security Management Forum (and IMT) is comprised of key leadership and technical expertise that operates holistically to establish sensible and effective policies, plans, and protocols, as well as pre-empt risk issues across the program. The SMP mission statement is to:

*Provide a safe and productive operating environment for staff where risks are identified and either avoided or appropriately mitigated before they occur, or where emergencies are managed in an effective and professional manner.*

#### I.3 Structuring Teams

SSFP should seek to create two organizations within its MBL operations at the earliest opportunity.

These teams include:

- A Security Forum
- An IMT

Membership of the team may be replicated, and duplication of roles may occur. The teams have distinct roles:

- Security management: To create and implement risk management strategies for protecting staff and assets, whether during travel or while at base location
- Incident management: To deal with the first minutes, hours, or days of a crisis at the local level to bring control and reduce crisis impacts

The structure of the security forum and incident management team for the respective lab is:

Function	Name	Contact No
Facility Security Manager		
Safety and Security Focal Person		
MBL Manager		
Incident Manager		
Logistics Manager		
Liaison Manager		
Technical Guidance		

**Remarks:** Additional appointments can be added, or a non-applicable (NA) can be annotated if the role is not required for this project. The facility security manager (in charge of the facility where MBL is parked) takes the lead role in security and incident management with administrative backup from the local security staff, oversight from National Institute of Health (NIH), and technical security guidance from GHSC-PSM BRD on a need basis. Training is also provided by FSM for the IMT periodically; records are retained.

The BRD contacts for technical guidance to the IMT during a crisis are:

Name	Appointment	Email	Phone

The crisis hotline number located at NIH details is:

Number

#### 1.4 Accountability

Work in the health environment can be rewarding but will always be challenging, and at times may expose personnel to risk. It is critical to the safety of the entire team that each staff member follow the guidelines and instructions contained within this document. Failure to comply with these security procedures may compromise not only an individual’s safety but also the safety of others.

SSFPs are responsible for supporting this plan and for leading through example. No deviations should occur based on status from the guidelines and instructions provided within this plan. SSFPs are also responsible for applying common sense and for taking the initiative for security and safety-related matters. If a SSFP or staff members perceive a significant risk associated with an activity, it is their responsibility to alert the management team and to stop any activity that might present a physical hazard.

**Remarks:** All non-compliance of security related instructions are to be reported to the FSM. Specific incident-related reports are kept on file with the NIH. Records are retained for future reference.

## 1.5 Networking and Leveraging

The FSM needs to establish strong relationships, where possible and appropriate, with local community, law enforcement agencies, other partners, and government groups and leadership. This will support a healthy sharing of information, as well as the management of an emergency.

The following relationships will be created to support BML operations:

Organization Name	Contact Name	Contact No

**Remarks:** *The FSM ensures that lines of communication are kept open within a wide warden network, such as an interface with local military and police contacts, ensuring information is collected and disseminated as quickly as possible. Local media are constantly monitored for further updates.*

## 1.6 Information Security

Staff should understand that every team member is a stakeholder within security management. Each person, regardless of status, has a role to play within ensuring safe and productive business. However, in some environments, sharing this plan and other details with all staff may be unrealistic, may compromise the safety and wellbeing of staff, or may expose others to unnecessary risk. As such, this plan will be shared only with the following groups and individuals:

Position	Name

The following requirements apply to MBL:

- All sensitive information is shredded or burned by SSFP.

*The SSFP is advised to procure a shredding machine and conduct periodic spot checks of team member workspaces to ensure sensitive information is locked away and correctly disposed of.*

The following risk mitigation measures are recommended for the MBL:

- Do not leave sensitive materials unattended, especially overnight
- Do not take laptops to areas prone to theft
- Sanitize IT equipment if espionage or removal of the materials might happen
- Keys should never be left unattended

## 1.7 Risk Coding

To support some degree of consistency in determining risk parameters, the risks prevalent within a particular operating environment or associated with a specific MBL operations need to be evaluated. Risks are fluid and complex, and as such, MBL operating within a high-risk environment may face less risks if operating in a certain manner or profile than a high-profile operation within a lower-risk environment. Using the basic system for

assessing information reliability and the probability of a threat occurring against the MBL, the following codes are applied to illustrate the risk coding for Pakistan.

<b>Code 1</b>	Security concerns exist, but they are typical in an operating context and are consistent with standard risks faced within Pakistan. The environment is considered permissive due to stable government and rule of law, and law enforcement or emergency responses are effective and reliable. Normal security management guidelines are adequate to address country-specific concerns. No specific tabletop assessment is required. No outsourced support services are typically required for risk management.
<b>Code 2</b>	Higher than normal (specific) security concerns exist, requiring a preliminary assessment of unique or amplified risks associated within the operating region. A basic risk management plan of how the security risks will be mitigated is required involving short-term support services from a security manager to evaluate the probability and impacts of postulated risks. Security concerns could exist in a specific region(s) or might be countrywide. A degree of political or cultural unrest may be prevalent within the region, or a lack of basic support infrastructures. Some higher levels of specific risks may be identified, such as crime, terrorism, or natural risks, such as health issues or earthquake threats. Common risks are amplified due to the inability of government or support services to respond to the risks.
<b>Code 3</b>	Serious (specific) security concerns exist that are either local or national in scope. A more detailed appraisal of how these risks impact the MBL operations is required to determine whether to continue operations. Dedicated security resources may be required to offset threats to MBL, whether these are policies and plans, or human and material resources. A more detailed tabletop assessment is likely required, followed by a pre-deployment field assessment for some operating environments. Specialist risk and planning advisory services are required, as well as a subcontracted local security company. Specialized security management plans may be needed at the beginning of operations, and arrangements, such as staff training, facility selection, and guard services are vetted through the security manager. Management may decide that security risks are too high for the MBL to be engaged in specific operations.
<b>Code 4</b>	A myriad of risk factors is prevalent within the operating country. Risks are considered high to extreme, and special threat management practices and resources are required. Typically, a post-conflict or conflict environment where ongoing human-created risks may target the MBL or staff specifically, or where natural risks are at a level where government is unable to adequately manage threats. Special security measures are required for the movement and protection of personnel, typically involving security transport and trained security professionals. Detailed risk advisory services are needed throughout the operations to identify and offset risks. Not all risks can be mitigated against, and residual threats are still likely to impact staff. Management may consider security risks to be too high for MBL to be engaged during that defined period or may require extraordinary security measures to enable operations.

These risk codes are applied against the Security Management Plan Index to suggest which elements should be applied. Local conditions and unique nuances may require modifications to this approach.

The risk coding for this plan is:

### 1.8 Risk Rating

The risk ratings applicable for this operating environment are assessed based on general threat evaluations. Specific events, periods, or incidents may quickly alter these ratings, either for short or extended periods of time:

Threat Nature	S	H	M	L
Robbery	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Theft and Pilfering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Burglary	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Road Traffic Accidents	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Assaults	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Carjacking	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Arrest and Detention	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fraud and Corruption	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Intimidation and Extortion	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Political Instability	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Workplace Violence	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ethnic or Religious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Terrorism and Militancy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Civil Disturbances	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Gangs and Sects	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Pandemics	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Storms	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Flooding and Tsunamis	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dust and Sandstorms	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Forest and Bush Fires	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Earthquakes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Chemicals Spills	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remarks: It is recommended that SSFM/FSM seek the counsel of the BRD to receive specific advice and measures to mitigate risk because the ratings are fluid and the situation on the ground can change with little or no warning. The final responsibility to determine risk and mitigation measures for MBL lies with FSM.

### 1.9 Crisis Management Decision Making

In an emergency, multiple areas must be managed:

1. How can I deal with the immediate physical and psychological harm to the staff?
2. How can I avoid more threats from harming the staff?
3. How can I let FSM and management know what is going on, so they can help me?

It is important to determine which individual is permitted to sanction certain actions to take place in terms of security practices or crisis management, or to determine which resources can be mobilized. The following Decision Matrix has been designed to empower MBL to make fast and effective decisions, or to liaise with the correct decision-making personnel.

### 1.10 MBL Branding

The branding for the MBL may be subject to scrutiny from external groups. Branding can expose the lab and staff to unnecessary risks and as such, careful consideration to official and unofficial branding should be given.

As such the following branding approach will be used:

- Branding Approach:
- Branding Logos:
- Branding Name:

## 1.11 Management Structures

### The Security Management Team

The security management team is comprised of a dedicated facility security manager, safety and security focal person, and other resources to ensure the safety and security of the staff and assets. The GHSC-PSM BRD team is available for technical guidance on security matters as a secondary function.

**Key Positions:** The following key positions are in place for the management structure:

Position	Name

## 1.12 Reports and Returns

Reports and returns are to be established to ensure that security-related information is passed both within the group, as well as to external groups and individuals authorized to receive this information.

Reports and Return Management is captured under the Security Plan Index section of this policy document. The reports and returns required for this MBL operations are:

- Serious Incident Report: Following an incident
- Accident Report: Following an accident
- Threat Alerts: When a threat has been sighted or reported
- Incident Report: When an incident occurs
- Information Compromise Report: When assets are stolen, copied or lost
- Discipline Report: When a disciplinary matter occurs
- Weekly Report: Addressing security issues
- Field Activity Report: An assessment of upcoming field deployment activities
- Facility Assessment Report: Security reviews of new or existing facilities as well as temporary locations

## 1.13 Legal Requirements

Staff must understand legal requirements for the MBL. As a rule, personnel are not to discuss or share material with external groups or individuals.

### Specific Agreement of Task Area

- Non-Disclosures Agreements:
- Teaming Agreements:
- Legal Resources:

The following unique laws or customs exist for this operating region:

#### 1.14 Security Management Roles and Responsibilities

▪ Director, Security	Responsible for establishing a security team, which might comprise security professionals (internal and external) as well as supporting managers who might be involved in risk management practices or support functions. Will be responsible for sanctioning strategic or operational decisions and ensuring the policies, plans, and protocols are maintained and implemented. <b>Remarks: Security Manager NIH</b>
▪ Security Manager	Responsible for offering expert advice and guidance on security-related matters and for evaluating risks and solutions associated with MBL operating methodologies, travel management, facility selection and protection, event management, and safety and security training. Also, responsible for overseeing all security personnel, and those involved in undertaking roles associated with safety and security. <b>Remarks: Facility Security Manager</b>
▪ Travel/Admin Manager	Responsible for coordinating travel arrangements, ensuring the correct travel protocols have been implemented and carried out. <b>Remarks: SSFP &amp; FSM</b>
▪ Human Resources	Responsible for ensuring all staff adhere to the security and safety policies and plans and coordinating safety and security training, in attendance and record-keeping. <b>Remarks: SSFP</b>
▪ Travel Security	Responsible for planning and managing travel of MBL, including aligning security and safety needs and resources with MBL activities. <b>Remarks: FSM</b>
▪ Training Manager	Responsible for ensuring that staff and security personnel receive the correct safety and security training as it benefits their role, as well as exposure to different risks. May retain records and coordinate training requirements with other managers. <b>Remarks: FSM</b>
▪ Liaison Manager	Responsible for establishing and coordinating relationships with external groups, agencies, and personalities to leverage the knowledge and resources of external parties for the betterment of MBL operations and staff. <b>Remarks: SSFP</b>

## SECTION II

### RISK MANAGEMENT

#### 2.1 Risk Methodology

MBL management and staff should understand that threat perception varies, and threat perception and tolerance levels may be much different from an individual within a field team. Also, various levels of experience and knowledge may result in far different perceptions and tolerance levels within the same team. As such, a standardization of what is considered acceptable is required to best protect members of a group, as well as MBL operations. Risks to staff, operations, and assets come in varied levels of probability and impacts, ranging from low, where the probability of situation occurring is highly unlikely, to extreme, where MBL should expect a risk to occur at some stage. The impacts associated with such events may be insignificant to extreme. By clearly defining probability and impact category levels, FSM will quickly come to understand the evaluated probability occurring within the lifespan of an activity. Some examples are provided as a basic guideline:





**Low Risk.** The probability of a risk occurring is unlikely and no special or costly measures should be implemented other than standard policies and procedures—unless the risk nature has a significant impact on MBL. A detailed Security Management Plan may not be needed, and risk awareness training may be useful only once a year.

**Medium Risk.** The probability of a risk occurring is possible and risk mitigation measures should be reflective of the costs and impacts such events will have upon MBL. These considerations will be reflected within the security and crisis management plans. Low-level management training will be beneficial to staff annually or biannually.


**High Risk.** The probability of a risk occurring is likely; as such, FSMs are advised to establish an appropriate budget to develop policies and procedures for counteract the probability of the risk occurring, as well as the subsequent impacts within the risk management methodologies. Thorough training will support management in responding to any emergency event more effectively, on a biannual or regular basis.

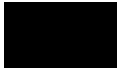
**Extreme Risk.** The probability of a risk occurring is certain to occur at some stage of the MBL. As such, FSM should consider whether to continue with lab operations, or acknowledge the impacts and responses within a detailed and tailored section of the risk and security management plans, with frequent and detailed tabletop exercises for varied levels of the management structure. Policies and plans should be connected to external organizations, and agencies and be tested and evaluated on a scheduled basis.


Probability and impact levels should be clinically evaluated to remove ambiguity or subjectivity undermining an effective assessment of the risk. The following table illustrates how MBL should define the likelihood of an event occurring, as well as the possible impacts the event might have.

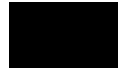
Level	Probability	Level	Impact
	The probability of an event occurring is considered low to remote.		The impacts are short lived and localized, not significant in scope.
	The probability of an event occurring is considered possible.		The impacts are significant but limited and often localized.



 The probability of an event occurring is considered likely.

 The probability of an event occurring is high or is expected to occur.

 The impacts are serious and may have long-lasting effects.

 The impacts are catastrophic, affecting every aspect of the company.

Remarks: *The level and probability of risks associated to the staff and assets in Pakistan vary greatly from area to area. Risk grading is performed by the FSM as events unfold, or on a weekly basis (whichever occurs first).*

## 2.2 Risk Registry

Staff and management must understand the risks associated with travel so that they can better understand the spectrum of challenges and threats—responding appropriately to identify, avoid, or mitigate these risks. The following risk considerations apply directly to travel:

Method	Risk Factor	Considerations
Land	▪ Road traffic accidents	Safety management practices
	▪ Criminal or terrorist targeting	Planning, awareness, and trend avoidance
	▪ Accident legal implications	Self-drive versus driver options

The following general risks are associated with MBL operations. By understanding the forms of risks associated with travel, staff are better placed to understand threats presented by travel, and to identify and navigate these risks more effectively:

▪ <b>Road Traffic Accident</b>	The collision of a vehicle with another vehicle, pedestrian, or object that results in injuries to the driver, occupants, or others, as well as damages to property or livestock
▪ <b>Hostile Families or Groups</b>	The involvement of loved ones, families, or social groups in association with an accident that presents physical or psychological risks to the driver or vehicle occupants
▪ <b>Hijacking and Hostage Situations</b>	The hijacking of groups of persons while traveling in vehicles—with the intention of illegally holding persons against their will for criminal, political, or terrorist-related reasons
▪ <b>Kidnapping</b>	The detention against a person’s will for criminal, political, or terrorist-related reasons, for individuals or small groups of travelers

▪ <b>Carjacking</b>	The theft of a vehicle, and possibly its passengers, for criminal gain
▪ <b>Theft and Robbery</b>	The removal of possessions or monies from individuals through threat, intimidation, misrepresentation, or the physical taking of materials for criminal or commercial gain
▪ <b>Delays and Stranding</b>	Risks presented to travelers resulting from a form of transportation being delayed or inoperable, leaving persons stranded in remote or high-risk areas
▪ <b>Explosive Devices</b>	The use of explosive devices on or against vehicles or other forms of transportation with the intent to damage property or injure travelers
▪ <b>Surveillance</b>	The observation or tracking of persons in connection to espionage or the intent to detain or harm persons or groups or to impact activities
▪ <b>Small Arms Fire</b>	The use of firearms against transportation or travelers with the intent to create fear or inflict harm
▪ <b>Detention and Arrest</b>	The temporary or long-term imprisonment of persons for alleged or actual crimes
▪ <b>Coercion or Intimidation</b>	The threat or use of violence to coerce individuals to act against persons, the group, or goals of the organization

**Remarks:** Training, briefing, verbal staff security updates, email, and SMS alerts are all methods used to keep staff up to speed on general and specific risks.

## 2.3 Risk Assessments

A comprehensive risk assessment is to be conducted to identify potential risks to the staff and assets. Perception plays a large part in how we view risk, either individually or as a group. This is because risk perception involves people's beliefs, attitudes, judgments, and feelings, as well as social or cultural values and dispositions that people adopt toward different hazards and their impacts. Simplistically, the subjective evaluation of risk can be separated into two categories:

- Objective risk evaluations. Evaluations of the potential for threats to occur based on facts, statistical data, and numerical methods.
- Subjective risk evaluations. Evaluations of the potential for threats to occur based on perceptions or a manager's professional opinion, in-country experience, etc.

Risks are fluid and can change rapidly due to unforeseen circumstances; however, by structuring a risk evaluation framework, management can better place risks into an understandable context. Such risk evaluations are complex, and subjective assessments and clear and consistent matrixes for evaluating impact and probabilities are required to evaluate and present a balanced risk picture. By conducting such evaluations, FSMs can more clearly identify where their greatest risks may lay, as well as where finite resources should be focused to mitigate such threats to personnel or general activities. Risk evaluations can be conducted at a strategic level to gain a macro perspective of where these challenges may lay, but should also be conducted at a local level, as the risk landscape may differ significantly from province to province, and in some instances, from neighborhood to

neighborhood. FSMs should also consider the following points when mapping and assessing these forms of risks for their areas of responsibility:

- **Hard and Soft Targets:** Is the MBL an easy target compared to similar assets/operations within the region, or are hostile groups more likely to achieve success focusing on less protected assets?
- **Incentives and Objectives:** What are the incentives and objectives of hostile individuals or groups—what are they trying to achieve, and how might they best achieve their goals?
- **Capabilities and Trends:** What are the realistic capabilities of hostile individuals or groups—do they have the knowledge, technology, and funding to be successful, or are they unable to launch sophisticated attacks? Do any trends support this analysis, or suggest future risks?
- **Mitigation Reliability.** What mitigation measures have been created to deal with such threats against MBL and our personnel? What gaps remain, and how effective are the measures? Should gaps then be addressed, or only acknowledged?
- **Impact Evaluations.** What impacts will be associated with risk events, to staff and to surrounding areas and populace? Consider the holistic impacts and ramifications of each risk type.

An important aspect of safe and productive MBL operations is the ability to identify and evaluate security risks before they occur. Depending on the operating environment and activities, the following steps may be taken to identify and manage risks:

- **Intelligence Assessments:** Gathering information from open or personal sources as to the threats that may face a person, location, or activity. These should not be based on rumor or speculation, but on solid fact or unbiased and reliable professional opinions.
- **Threat Assessments:** Evaluating intelligence against the activity and risks and determining the probability and impacts of possible risks from occurring, as well as possible mitigation measures.
- **Security Surveys:** Reviewing sites and activities to place intelligence reviews and threat assessments into a granular context and developing approaches or strategies for enabling safe and productive work to occur.
- **Security Plans:** Designing a specific approach plan for an activity or site to mitigate threats identified within the intelligence reviews, threat assessments, and security surveys. This includes the staff and resource levels required.
- **Security Audits and Assessments:** Reviewing existing security measures to ensure they are consistent with the needs in terms of threats and the way the MBL is operating.
- **Individual Risk Assessments:** Evaluations of specific individual risks based on unique threats, such as intimidation, specific targeting, or surveillance.
- **High-Risk Travel Assessments:** Conducting specific evaluations for high-risk or long-distance road, or other, movements to identify and mitigate risks.
- **Threat or Trend Tracking:** Tracking trends, both internally (such as common trips and associated risks) or externally (such as the targeting of similar groups), to identify a pattern and possible impacts against the MBL and staff.
- **Risk Mapping:** Capturing threats within maps or other tools to better illustrate potential risks against the MBL and staff.

## 2.4 Minimal Security Standards

Minimal and consistent operating practices within MBP operations are needed to establish clear operating parameters for staff. These standards should be applied by all staff, regardless of experience or position.

- Internal: Standards developed within the MBL to reflect best practices to mitigate potential risks
- External: Standards set outside the MBL, which define best practices, such as government bodies or industry standards

**Remarks:** Minimal security standards vary greatly between the MBL deployed locations. Lahore and Karachi, Islamabad, and Quetta each have unique standards. Training and continuous evaluations of staff and processes occur to ensure standards are maintained.

## 2.5 Information Security

Information security is a responsibility of management and staff. Carelessness with sensitive information enables unsavory individuals or groups to either directly or indirectly target staff, facilities, or activities. As such, strict information security measures should be adopted, including

- **Security Protocols:** Staff should not share security protocols or procedures outside of authorized personnel.
- **Data Management:** Data management should be carefully controlled—disused IT or hard-copy information should be destroyed or sanitized.
- **Information Restrictions:** Clear “need to know” policies should be developed and sustained.
- **Personal Details:** Personal details, especially for local staff, should be protected.
- **Event Information:** Details pertaining to key events should be guarded and shared only with those requiring the information.

The following is considered sensitive or restricted information:

- Security Management Plan
- Incident Management Plan
- Facility Security Plan
- Travel plans and itineraries
- Event plans and documents
- Operating policies and work plan
- MBL papers and documents

## 2.6 Incident Management and Crisis Response

The Security Management Plan deals with local-level crisis management requirements, enabling the MBL team to move through the first minutes and hours of an emergency event, as national resources and expertise are mobilized.

**Incident Management Plans:** Immediate response drills and protocols to help local SSFP to respond to immediate threats.

Staff should refer to the Incident Management Plan for guidelines on how to manage specific crisis events at a personal and group level.

**Remarks:** Immediate response drills are posted on the MBL wall and staff are offered biannual training by FSM to ensure wide understanding of standing protocols. Incident management is conducted according to defined training and policies.

## 2.7 Relocation of Critical Functions

Under exceptional circumstances the MBL may need to relocate due to a crisis event. This may require some staff to work from alternative sites or to adopt a “work from home” policy.

## Consideration

## Alternative

- Relocate MBL functions
- Relocate on a district level
- Relocate on a provincial level

## 2.8 Personal and Management Conduct

Personal conduct is a fundamental aspect of an effective Security Management Plan; as such, all staff must adhere to sensible policies and protocols for reducing personal risk within a remote, new, or challenged operating environment.

The following basic principles should be applied:

- Keep a low profile and demonstrate respect for others.
- Communicate respect through your listening skills and non-aggressive body language.
- Accept criticism and the legitimacy of others' viewpoints.
- Be aware and respectful of local political, religious, and cultural sensitivities.
- Do not dress in a way that attracts attention.
- Avoid large public gatherings, especially demonstrations and political rallies.
- Avoid locations known to be dangerous or unstable.
- Do not bribe officials or offer gratuities to officials for carrying out their work.
- Do not provide opportunities for theft. Do not display cash or material goods.
- Do not carry cameras or take photographs in areas where security is unstable.
- Be careful not to offend local customs or when taking pictures.
- Do not take any photos in or around military installations and checkpoints.
- Be sensitive to cultural gender issues
- Be aware of public events that might present risks.
- Watch the news and check government websites for alerts or warnings.

SSFP must set examples to junior staff regarding security and safety practices. SSFP will be held accountable for any deviations that might undermine the principles of safe operational or personal conduct within the MBL. This also relates to visiting short-term staff. SSFP will:

- Adhere to the guidelines, directives, and instructions within this plan.
- Ensure security staff deliver services and conduct themselves to the standards of the plan.
- Encourage and where needed enforce the principles and directives of the plan.
- Report incidents or occasions where deviations of the requirements of the plan occurs.
- Identify and recommend methods by which to improve and evolve the plan.

## Section III

### OPERATIONAL SECURITY

The provision of established and documented security policies, protocols, and plans brings greater consistency to managing risk and supports more effective management practices.

#### 3.1 Security Controls

Security controls are needed to support a more organized approach to risk and security management. These include:

**Risk Criteria:** This document has established some basic security criteria to help FSMs understand what standards should be adopted across MBL operations.

- **Parked Location:** minimal security standards: Minimal security standard matrixes have been created to help management select appropriate and sustainable locations for long-term parking of labs. FSMs should determine what nuances may applied to each office location and document specific security policies or approaches.
- **Mobile Location:** minimal security standards: Minimal security matrixes have been created to help management select appropriate and sustainable locations for temporary parking of mobile labs in the field. FSMs should determine what nuances may applied to each office location and document specific security policies or approaches.

For all parking requirements, the question is to determine if the facility selected is appropriate given the risk environment, and what the probability is of a crisis event occurring, as well as the potential impacts. Staff should be aware that high-profile sites or occupants may raise their profile and expose them to unacceptable levels of risk, but that robust security measures may counterbalance high-profile sites. As such, a careful balance of security and profile should be weighed.

- **Intelligence Processes and Management:** The FSM is responsible for mapping and exploiting open and personal networks of information sources—supported by all staff—to identify and mitigate risks.
- **Risk Consulting:** Management staff should separate security management from risk consulting. Management is the coordination of resources and activities; risk consulting is the strategic planning of risk management. Both functions complement each other to protect staff, operations, and assets.
- **Security Management:** Security management is the practical operational planning and tactical management of risks for project staff, activities, and assets.
- **Investigations:** Investigations are sensitive matters and should be conducted only with the correct authority from appointed management. No local management or staff should conduct investigations without seeking approval from authorized leadership through the management chain.
- **Due Diligence:** Due diligence should be conducted for employed staff and contracted vendors, etc. A vetting system may be required to ensure that the correct due diligence is conducted and that such checks are evidenced within a formal document.
- **Disciplinary Issues:** Security management also involves correctly managing disciplinary issues and dealing with matters in a manner that does not exacerbate a problem or expose management or other staff to risk. For serious issues such as fraud, corruption, serious theft, and sexual harassment, the SSFP should advise the FSM before acting.
- **Warden List:** SSFP should establish a Warden List that tracks vulnerable persons and supports a cascade process of tracking staff during an emergency, of disseminating emergency information quickly and effectively.

## 3.2 Travel Management

All movement by the MBL will be managed through a robust and comprehensive travel management plan. A detailed risk assessment will be conducted before each travel by the FSM and SSFP, advised by appropriate risk mitigation measures. At a minimum the following areas will be covered:

- **City Risk Index:** The city risk index tracks risks associated with both cities where operations occur, as well as common higher-risk or longer-distance routes.
- **Historical Risk Tracker:** A historical risk tracker may be required where MBL is visiting higher-risk locations, often to control pattern setting.
- **Individual Task Assessment:** For high-risk trips a specific trip risk assessment should be conducted to identify risks, plan mitigations, and reevaluate threats to staff to determine a methodology of risk management, as well as identify when threat tolerance levels have been breached.

The minimal standards for this project (as a general approach) are:

- Trained drivers in safety and security
- Travel risk planning conducted
- Security escorts (armed) used
- Tracking devices used in vehicle coordination with military or police
- Satellite phones carried
- Medical/trauma packs carried

An evacuation plan for staff and assets needs to be made for each location, as it is an important aspect of emergency preparedness.

For sites or areas where staff operate frequently or for protracted periods, the FSM needs to have local evacuation plans that support the immediate protection and extraction of staff from an affected area.

## 3.3 Location Security

Security measures for locations are important, as they are where staff and assets are vulnerable due to being focalized and static targets for unsavory individuals and groups. As such, location protection is a fundamental aspect of security management:

- **Security Staff:** Facility security may involve providing facility guards and shift leaders. It is important that the right levels of security staff are selected to meet the needs of access control, patrolling, lock and key security, and response.
- **Security Escorts:** Security escorts are staff who escort visitors to and from MBL and ensure they are monitored and arrive and depart from their visit areas.
- **Security Structures:** The FSM must strike the right balance between profile and a robust structural security plan that delays, detects, and prevents intruders from gaining access to a site area holding MBL.
- **Perimeter Security:** Perimeter security may be either a physical or psychological barrier and provides a clearly marked barrier or demarcation between public and nonpublic areas. Perimeter security measures should reflect the local environmental conditions, as well as profile.
- **Access Control:** Access control points are typically the weakest point within a facility security plan, as they permit entry for vehicles and pedestrians. The threats of persons seeking to enter, or force entry, into the site should be evaluated, and adequate access control measures be sought to restrict entry.
- **Lost Keys:** Locks for lost keys should be replaced immediately to ensure that locks cannot be compromised.
- **Searching:** The searching of people and vehicles, whether blanket or spot checking, is often required within higher-risk environments, both upon entry and exit, to ensure persons are not bringing

unauthorized items near MBL or taking items from the MBL. This can be a cultural, status, and gender-sensitive issue.

- **Doors:** Doors should be strengthened within higher-risk environments to provide a temporary or robust barrier between staff and those seeking unauthorized access.
- **Windows:** All windows must have tempered glass and be secured through iron bars.
- **Blast Film (Windows):** Within environments where explosive hazards occur, FSM should consider having windows fitted with blast film to reduce fragmentation hazards.
- **Safe Havens:** A haven is a room or area that provides temporary or longer-term security and safety from manmade risks within a compound. Safe havens will be identified by FSMs for each operating region.
- **Security Technologies:** The use of CCTV, intruder detection systems, and badging control measures can increase security measures while reducing profile and manpower levels. The sensible balance of technologies and manpower levels are defined for each MBL.
- **Security Lighting:** Security lighting is used to deter or detect intruders, although it raises the profile of MBL. Sufficient lighting will be provided as required.
- **Security Protocols:** Security protocols that define how MBL will be secured is required to ensure that guards and occupants adhere to practices that support sensible security measures.
- **Lock and Key Security:** All staff should be aware of lock and key security, including locking sensitive items during or after use and ensuring that lost or missing keys are immediately reported so that new locks can be fitted.

The following minimal standards will be applied for facilities holding long-term parking (LT) and temporary parking (TM).

<b>LT</b>	<b>TM</b>	<b>Minimal Standards</b>	<b>LT</b>	<b>TM</b>	<b>Minimal Standards</b>
<input type="checkbox"/>	<input type="checkbox"/>	Vehicle access control gates	<input type="checkbox"/>	<input type="checkbox"/>	Security lighting
<input type="checkbox"/>	<input type="checkbox"/>	Boom barrier or hydraulic ram	<input type="checkbox"/>	<input type="checkbox"/>	Bars on windows
<input type="checkbox"/>	<input type="checkbox"/>	Pedestrian access control doors	<input type="checkbox"/>	<input type="checkbox"/>	Outer security doors
<input type="checkbox"/>	<input type="checkbox"/>	Perimeter walls	<input type="checkbox"/>	<input type="checkbox"/>	Inner security doors
<input type="checkbox"/>	<input type="checkbox"/>	Anti-climb devices (walls)	<input type="checkbox"/>	<input type="checkbox"/>	Panic alarms
<input type="checkbox"/>	<input type="checkbox"/>	Intruder detection systems	<input type="checkbox"/>	<input type="checkbox"/>	Fire alarms
<input type="checkbox"/>	<input type="checkbox"/>	CCTV	<input type="checkbox"/>	<input type="checkbox"/>	A haven or room
<input type="checkbox"/>	<input type="checkbox"/>	Electronic access keys	<input type="checkbox"/>	<input type="checkbox"/>	Medical packs
<input type="checkbox"/>	<input type="checkbox"/>	Badging controls	<input type="checkbox"/>	<input type="checkbox"/>	Security escorts
<input type="checkbox"/>	<input type="checkbox"/>	Unarmed guards	<input type="checkbox"/>	<input type="checkbox"/>	Bag and luggage spot checks
<input type="checkbox"/>	<input type="checkbox"/>	Armed guards	<input type="checkbox"/>	<input type="checkbox"/>	Guard patrols (facility and grounds)
<input type="checkbox"/>	<input type="checkbox"/>	Visitor sign-in registry	<input type="checkbox"/>	<input type="checkbox"/>	Vehicle searches
<input type="checkbox"/>	<input type="checkbox"/>	Laptop sign-in registry	<input type="checkbox"/>	<input type="checkbox"/>	Pedestrian searches (male/female)
<input type="checkbox"/>	<input type="checkbox"/>	Vehicle search mirrors	<input type="checkbox"/>	<input type="checkbox"/>	Search wands



- |                          |                          |                           |                          |                          |                    |
|--------------------------|--------------------------|---------------------------|--------------------------|--------------------------|--------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | Metal detectors           | <input type="checkbox"/> | <input type="checkbox"/> | Fire extinguishers |
| <input type="checkbox"/> | <input type="checkbox"/> | Blast film for windows    | <input type="checkbox"/> | <input type="checkbox"/> | Panic alarms       |
| <input type="checkbox"/> | <input type="checkbox"/> | Phone entry restrictions  | <input type="checkbox"/> | <input type="checkbox"/> | Clear desk policy  |
| <input type="checkbox"/> | <input type="checkbox"/> | Guards have mobile phones | <input type="checkbox"/> | <input type="checkbox"/> | Guards have radios |

Alarms will be:  Silent  Audible  Linked to the police  Linked to private security.

*Remarks: Each MBL should have two different audible alarms. One alarm sounds during a fire/hazard, and the other sounds in the event of an attack. The audible system is to be routinely tested, and biannual drills are conducted to ensure that all staff are familiar with the alarm soundings and the immediate actions to be taken.*

Working late within a MBL can present unique challenges:

MBL policy on working outside office hours is:

### 3.4 Temporary Parking: Location Security

The FSM needs to identify and address the multitude of threats presented to staff, assets, and visitors, including considerations such as the following for all short-term field locations identified to host the MBL.

- **The Venue:** The risks associated with the venue, both in terms of direct threats as well as peripheral threats from adjoining locations, should be considered.
- **Routes to the Venue:** FSM should consider the threats associated with traveling to and from the venue site, during set-up and demobilization as well as during the deployment itself.
- **Staging Areas:** FSM should consider risks presented at staging areas, such as hotels where staff are staying during the deployment period.
- **Profile:** The profile of the venue site, other activities ongoing, as well as visitors and the nature of the deployment should be considered to determine whether the location will draw unreasonable levels of risk.
- **Security Measures:** The organic security measures in place at the venue site, as well as those provided by commercial and government supporting agencies, should be considered to determine whether these reflect the risk tolerance as well as the risk environment in which the deployment is taking place.

### 3.5 Investigations

The investigation of thefts, threats, or other matters can be sensitive and present security and safety risks for staff as well as the MBL operations. Also, inappropriate investigations or unlawful actions can present legal and reputational risks. The following considerations should be applied before an investigation is conducted:

- Is it legal to investigate?
- Will an internal investigation compromise evidence and any subsequent charges?
- What security implications may be associated with an investigation?
- Who might be targeted because of an investigation?
- What moral or ethical considerations are associated with the investigation?

- Who is best placed to investigate (internal or external)?
- Should the local police or other agencies be involved?
- What actions will be taken if evidence is found?

### 3.6 Threats and Extortion

In some areas of Pakistan, threats may be made to coerce or extort staff. Often, threats are unfounded and not followed through. However, in some instances, threats might result in physical and psychological harm. If threats are made by known persons publicly, FSMs will be better placed to deal with the matter. If the threat is made by unknown persons, determine the following factors:

- What threats are being made; what impacts, and threats are there?
- What is the probability of the threat being carried out?
- Who might be making the threat? Can likely perpetrators be short-listed?
- Can phone calls be triangulated using a phone company?
- Can emails be traced?
- Who answers the phone; can a ruse be used to gather information?
- Is there a trend or pattern to the threat?
- Might the threats be false or made by staff members as a ruse for self-gain?
- What security and safety risks are there?
- Should working and personal practices change?
- What training or advice might be required for targeted staff?
- What security resources and support might be needed?

Threats or workplace violence are to be reported

### 3.7 Pilfering and Theft

An important aspect of security for the MBL is preventing pilfering and theft. This includes protecting valuable items and information through lock and key security, as well as creating systems and protocols that reduce the chances of theft. The following methods apply:

- Bags will be searched when entering the facility.
- Spot check searches will be conducted of all staff.
- Spot check searches of vehicles will be conducted.
- Internal and compound CCTV cameras will be used to monitor thefts.
- Lockdown procedures will occur if thefts occur.
- An appointed person will search identified spaces for stolen items.

### 3.8 Communications

Effective communications are the foundation for security and incident management. The following general principles apply to ensure effective communications can occur:

- Phones must always be switched on
- Numbers will be pre-programmed into mobile phones
- Numbers will not have name or title listings, which might compromise staff
- Satellite phones will be issued to support effective communications
- The numbers for critical persons and services will be known by all staff
- SSFP will deputize critical functions if unavailable

The following key numbers will be shared with all staff:

Organization Name	Contact Name	Contact No.
Hotline		
Hospital		
Fire		
Ambulance		
Bomb Disposal		
Police		
Other		

The warden tree will record details of staff deployed with each MBL.

Warden	Group	Number

### 3.9 Medical Supplies

MLB may need medical supplies and stores to enable first-line treatment to be administered to injured or sick staff. The following medical stores should be provided:

LT	TM	Minimal Standards	LT	TM	Minimal Standards
		First Aid box			Defibrillator
		Stretcher			Advanced trauma pack

### 3.10 Recruitment and Vetting

Recruitment and vetting can be an important aspect of ensuring safety and security for the MBL operations. Management should consider what levels of vetting might be applied during recruitment: key staff might be vetting in more depth than those who do not hold critical roles or have access to sensitive information. The following vetting will be conducted:

Key Staff	General Staff	Others	Vetting Requirements
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic police background check
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Detailed police background check
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Private security background check
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Basic application checks required
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Full application checks required
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Physical background checks required

## SECTION IV

### EMERGENCY PREPAREDNESS

Preparing for crisis situations before they are underway provides opportunity to establish effective plans and responses before a disaster strikes; as such, we are better prepared to protect our staff and recover from a crisis event.

*Staff must adhere to the instructions of the Security Management Forum and guard force during a crisis.*

#### 4.1 Emergency Preparedness





This plan places immense value on emergency preparedness, ensuring that as a team it is best prepared to identify, mitigate, or deal with a crisis. By establishing sound contingency planning, individuals and groups are better prepared to manage emergency situations.

- **Incident Management Team Structures:** It is important to define the structure of the MBL incident management team, as well as responsibilities before the crisis occurs.
- **Roles and Responsibilities:** Clearly defined role and responsibilities should be established for the incident management team to avoid confusion and duplication of effort during the response to an emergency.
- **Incident Management Centers** (physical and virtual): NIH's IMC will act as a fusion point for management decision-making and congregation during an emergency.
- **Communications and Technologies:** The FSM should ensure that multiple means of communication are available to support communications should an emergency occur. At least three means should always be available (mobile, landline, and internet).

Remarks: The Operations Room has access to mobile phones, Internet, and CCTV.

#### 4.2 Alert States

The following Alert States have been provided to enable incident and crisis management responses to have a more defined structure for how a pending emergency event (alert) or an occurring event (incident) trigger defined response measures to reduce risks or control the impacts and implications of an emergency:

Alert	Grading	Reporting	Actions
	Low/negligible risk level	Rumors or speculations of possible minor events	Respond with low-level risk mitigation
	Medium levels of risk	Minor events occurring or reported to occur shortly	Initiate graduated risk and security responses
	Elevated levels of risk	Momentous events occurring or about to occur	Initiate security and crises management protocols
	Serious levels of risk	Catastrophic crises events occurring or imminent	Initiate full-scale security and crises response

Establishing tripwires or alerts and trigger points enables SSFP, as well as FSM, to have clearly defined and unambiguous points at which decisions or actions are taken, whether a major earthquake, large-scale riots, pandemic alerts, or fuel shortages and water contamination threats. These specific trigger points or tripwires can include:

- Demonstrations that indicate growing social unrest, whether peaceful or violent in nature; especially if aimed at foreign workers, facilities or other associated company activities
- The media, host government, religious groups or leadership, or militia leaders preaching or actively spreading inflammatory propaganda or directives that could adversely affect the MBL operations, its personnel or assets
- A rapidly diminishing ability to gain accurate and timely information from government organizations and media agencies on local or regional events that could present threats to staff or activities
- Increasing levels of opportunistic criminal activity; especially if directed at specific ethnic or religious groups, genders, business activities, locations or facilities
- Focused attention by organized crime on the MBL, its staff, activities; or unwanted attention toward associated or similar commercial groups
- Rising levels of insurgent, terrorist, or activist targeting; especially if directed toward MBL, or associated or parallel groups
- Country's public announcements indicating an increase in specific threat types, or pending crisis events
- Sustained disruptions to basic infrastructure or utilities preventing the supply of clean water, gas, electricity, food, fuels or other life support essentials
- Reliable reports of an imminent natural disaster; hurricane, wildfires, volcanic eruptions or flooding
- Reports of a pending or occurring industrial or environmental disaster that could present toxic or physical hazards to personnel, as well as contaminate facilities, food or water supplies or critical materials
- An outbreak of contagious diseases that the local government or responding agencies do not have the resources, expertise or medicines to treat
- Rapid economic decline brought about by sanctions, civil unrest, coups, assassinations, or the turnover in country leadership, which might lead to local authorities being unable to maintain law and order
- Political tensions from foreign governments, which might trigger country's political responses, presenting risks to ethnic, religious or national groups
- Political instability and loss of governance resulting from the abrupt replacement, detention or arrest of key government officials, military leaders, political opponents, religious leaders or other prominent figures
- Similar organizations increasing security profiles, ceasing operations, closing facilities, rapidly evacuating personnel or demobilizing activities
- Other agencies declaring heightened risk alerts or withdrawing their presence from the area, region
- The inability, lack of resources or unwillingness for local or national security and law enforcement agencies to provide adequate protection to MBL
- Rising levels of corruption, extortion, and legal liability risks presented by corrupt political leadership, which could result in detentions or imprisonment
- The guidelines should be considered as such, guidelines, with common sense playing a critical role in how SSFPs respond

### 4.3 Trigger Response Plans

It is important for staff to understand how alert states might trigger an organizational response to a particular kind of threat. Triggered response protocols ensure that defined and consistent actions are taken when alert states are issued—supporting individuals and the organization in knowing what measure to take to mitigate possible increases in risk.

Should the following crisis events occur, they will trigger an immediate notification of the incident management team as well as an immediate report (verbal then written) to the NIH Incident Management Center:

- |                                     |  |                                   |   |
|-------------------------------------|--|-----------------------------------|---|
| <input type="checkbox"/> Kidnapping | <input type="checkbox"/> Hostage       | <input type="checkbox"/> Fatality | <input type="checkbox"/> Significant Injury |
| <input type="checkbox"/> Assault    | <input type="checkbox"/> Armed Robbery | <input type="checkbox"/> Accident | <input type="checkbox"/> Facility Fire      |

- |  |   |  |   |
|--|---|--|---|
| <input type="checkbox"/> Fraud Incident        | <input type="checkbox"/> Intimidation     | <input type="checkbox"/> Arrest            | <input type="checkbox"/> Exit Denial    |
| <input type="checkbox"/> Political Instability | <input type="checkbox"/> Terrorist Attack | <input type="checkbox"/> Civil Disturbance | <input type="checkbox"/> Media Incident |
| <input type="checkbox"/> Workplace Violence    | <input type="checkbox"/> Major Flood      | <input type="checkbox"/> Earthquake        | <input type="checkbox"/> Pandemic       |
| <input type="checkbox"/> Major Storm           | <input type="checkbox"/> Landslip         |  |   |

The following Trigger Response Table illustrates the forms or triggered responses that might occur if alert states are issued or identified.

**LT Location:** Increase the security awareness of MBL staff and security personnel deployed. Ensure normal lock and key security measures are undertaken and test security procedures and technologies. Discuss security with the FSM to seek guidance.

**TM Location:** Conduct normal travel in the field while having greater awareness of security and higher-risk travel requirements. Review the need for additional mitigation measures if the situation worsens.

**Action:** Implement specific risk management protocols related to postulated threats at the local level. Notify the incident management team and review policies and protocols

**LT Location:** Security personnel are on a higher alert and conduct frequent patrols of the MBL area, securing non-essential access points. More searches to be conducted of vehicles and persons near the MBL. Secure MBL policy initiated, and personnel advised of postulated risks.

**TM Location:** All higher-risk travel stops without review of travel assessment for the affected areas. Potential escalation in risk factored in for developing mitigation measures. Review of risk and crises plans to ensure readiness to respond to incidents.

**Action:** Implement specific risk management protocols associated with specific risk level to staff. Notify IMT of actions taken.

**LT Location:** Secure access points and limit visitors, ensure current security personnel are alert, and conduct more thorough patrols and searches. Start standing down non-essential personnel. Test security measures and stand-up additional resources as required.

**TM Location:** Travel risk assessments conducted, and only vital or mission-essential travel conducted. Additional security considerations applied for travel and security resources allocated. Consider delaying deployment where possible until the situation improves.

**Action:** Implement risk management procedures and notify NIH for additional security support. Provide risk review and discuss probability levels and associated impact.

**LT Location:** Secure MBL by posting additional guards; evacuate non-essential personnel from the MBL. Cancel all operations. Assistance from law enforcement agencies to be sought.

**TM Location:** Travel is suspended with all staff relocated to a safe location. MBL is secured with additional guard force and if possible, moved to a secure compound. Assistance from law enforcement agencies to be sought.

**Action:** Implement crises management protocols. Engage law enforcement agencies and coordinate response with assistance from NIH and official agencies.

## 4.4 Alert Notifications

Security alerts are called when the safety of staff or assets is threatened. Examples of events that trigger a security alert include:

- Strategic or momentous events occur that could threaten staff safety
- Indications of possible threats are reported against staff, facilities, or activities
- Other similar groups are targeted within the area or region
- Trends of targeting similar or connected groups are identified by government alerts
- Reports from other organizations are received regarding possible threats
- Local staff report possible targeting or grounded concerns raised
- Surveillance is detected that may result in a criminal or terrorist attack
- An unusual or dangerous activity is occurring that could be the precursor to risks

in a security alert, all staff are expected to follow instructions from the Security Forum. An alert state will be issued as a formal report, or verbal warning.

The SSFP should create a warden system to locate staff during a crisis event. To ensure that alerts can be distributed effectively, the following rules apply:

- Phones must be always kept on
- Phones must have an adequate credit and have all numbers up to date.
- Group text alert systems will be created
- Group email alerts will be created
- Staff should have key numbers logged into the phone
- Training should be provided in using satellite phones

## 4.5 Incident Management Response

To support SSFP operating within a particular environment and to deal with emergency situations, an Incident Management Plan has been developed. It provides tailored management emergency response guidelines and information data and capture sheets to reflect the wide range of postulated risks the MBL might face, as this provides specific instructions to reflect the nuances of each risk type. There is also mileage in having a catch-all incident data call that meets the generic needs of those risks that might not have been anticipated; or span multiple areas. A standardized Serious Incident Report to document and manage information flow on any serious events occurring has been developed to capture all incidents, especially those with any impact on the MBL. This report will capture any relevant information should the specific incident response templates provided not match up to a unique event. The report should be completed and released during and after each serious incident; either to capture multiple risk natures or to reflect a gap in the project reporting templates.

Of primary importance to the SSFP responsibility is managing the series of incident management guidelines and information capture reports that have been developed to help staff verbally report an incident at the start of an event, as well as provide a checklist and associated information reports for individual risk types. The SSFP is responsible for ensuring staff are trained in using the verbal reporting system, understanding and using the management guidelines, and providing written reports using the pre-defined formats provided.

Staged reports to capture the details of a fluid event requiring initial, interim, and closure reports are required, especially as events evolve and further information is gained for distribution. All reports must be completed correctly and in sufficient detail, as they may be used for audit or investigation purposes. Within 48 hours of an event, a risk evaluation is also required to formally address direct and peripheral risks associated with the event. These tools and policies are found within the Incident Management Plan.

Serious incidents might include hostile incidents resulting in injury, death, or serious difficulties; severe injury or death from natural causes or accidents; serious industrial accidents or evacuations; serious legal or reputational situation; and the loss of a critical or high-value asset.

#### 4.6 Crisis Response

The ability of SSFP to respond to a crisis quickly and effectively, in a well-coordinated and pre-agreed way, will significantly affect how well individuals and groups navigate an emergency situation.

- **Crisis Communications:** A formal crisis communications plan is in place that indicates who is responsible for different functions. It is to be kept up to date and accurate and to be distributed.
- **Evacuation Management:** All appropriate staff have been briefed on the evacuation plans and are aware of where to find them and have access to the instructions they will need.
- **Medical Emergencies:** Suitable medical centers or support structures have been identified to support medical emergencies.
- **Kidnap and Ransom:** Staff have received kidnap and ransom training or advisory information. The incident management team and BRD understand how to manage a kidnap and ransom situation.
- **Fraud and Corruption:** Staff and managers understand the dangers associated with fraud and corruption in terms of individual and group risks—and how to report and manage such an event.
- **Extortion and Intimidation:** Staff and managers understand the dangers associated with extortion and intimidation in terms of individual and group risks—and how to report and manage such an event.
- **Media Management:** Staff and management are aware of the typical means by which media groups gather information—and how to respond to various forms of media interaction.
- **Earthquakes and Floods:** Staff and management are aware of how to respond to localized or widespread earthquake or flood events in terms of immediate response as well as post-incident management.
- **Pandemics:** Managers and staff understand how to prepare for and manage pandemic alerts and events in terms of work-from-home policies, isolation strategies, and hygiene arrangements.
- **Work-Place Violence:** Systems and protocols are in place to deal with workplace violence when operating remotely or in challenged regions where typical support structures are absent.
- **Stress Trauma Management:** Management understands the signs, symptoms, and first responses to stress trauma, for individuals and groups.



## SECTION V

### TRAINING AND EDUCATION

Training and education play an important part for SSFPs and staff in understanding how to manage risk, safety, and crisis events. Ideally, training should occur before or during deployment, or immediately upon beginning work. It is the responsibility of the FSM to ensure that training is delivered to SSFP, and all staff deployed on MBL. Staff should be proactive and request training if none is scheduled for them. This Security Management Plan prescribes facility-specific security training of the designated provincial facility security managers in the following areas of desired competencies.

#### 5.1 Awareness, Training, and Competency

FSMs should be aware of what training is required to best protect staff within different operating areas. Basic standards should be designed to meet minimal levels or requirements for each operating environment. This should address the requirements of the incident management team, as well as basic security and safety for staff functions.

- **Management Training:** The provision of leadership training in security, risk, and incident management skills.
- **Staff General Training:** The provision of safety and security training for all staff that reflects the generic risks faced within a particular operating region.
- **Specific Staff Training:** The provision of specific training to staff exposed to unique or targeted risks associated with their role, position, or functions.
- **Static Teams:** The provision of specific training related to staff working in fixed locations and targeted risks associated with their role, position, or functions.
- **Mobile Teams:** The provision of specific training related to staff working in the field and targeted risks associated with their role, position, or functions.

#### 5.2 Deployment Training

Where possible, pre-deployment training will be conducted, although this is problematic given the sporadic nature of deployments and the varied locations from which people deploy.

**Hostile Environment Training:** FSMs will provide security awareness training relating to high-risk environment covering:

- Personal safety and security
- Land-based travel safety and security
- Human-created risks and emergency responses
- Natural risks and emergency responses
- Cultural and social risk considerations
- Health and hygiene risk considerations
- Staff traveling to remote or higher-risk cities in country
- Local staff induction training to MBL
- Strategic events or situations
- Post-crisis incidents

Remarks: SSFP will be responsible for providing safety and security briefings to all new or visiting staff.

Pre-deployment

- Advisory Letters: Security advisory letter or document provided to staff before they depart their point of origin.

### 5.3 Specific Management Training Requirements

For environments where crisis events are more likely, it is useful for SSFPs to undertake either informal or formal training. Incident and crisis leadership training may involve discussion groups, tabletops, practical exercises, and open forums.

Applicable Subject Area	Frequency
<input type="checkbox"/> Incident management	As requested,
<input type="checkbox"/> Crisis leadership	As requested,
<input type="checkbox"/> Security management	As requested,
<input type="checkbox"/> Kidnap and ransom management	As requested,
<input type="checkbox"/> Fatality and repatriation management	As requested,
<input type="checkbox"/> Emergency evacuation management	As requested,
<input type="checkbox"/> Disaster response management	As requested,
<input type="checkbox"/> Pandemic response management	As requested,
<input type="checkbox"/> Arrest and detention arrest management	As requested,
<input type="checkbox"/> Extortion, intimidation and coercion management	As requested,
<input type="checkbox"/> Leveraging and networking	As requested,
<input type="checkbox"/> Guard force management	As requested,
<input type="checkbox"/> Analyzing and using information	As requested,
<input type="checkbox"/> Transportation security	As requested,
<input type="checkbox"/> Facility security	As requested,
<input type="checkbox"/> Event management security	As requested,
<input type="checkbox"/> Warden management	As requested,

## Annex 2: Incident Management Plan

Version 1.0

# Mobile Bio Laboratory



## INCIDENT MANAGEMENT PLAN

**Country**  
**Location**  
**MBL Tag No**  
**Team Leader**  
**Safety & Security Focal Person**  
**Security Manager**  
**Dated**  
**Review Date**  
**Custodian Name**  
**Appointment**

# MANAGEMENT RESPONSE GUIDELINES

- ❖ Introduction
- ❖ Security Management
- ❖ Goals and Objectives
- ❖ Risk Management
- ❖ Incident Management Plan
- ❖ Vehicle Physical Security Breach
- ❖ Small Arms Fire
- ❖ Hostage Situation
- ❖ Domestic Terrorism and Special Interest Group
- ❖ Site Occupation and Sit-Ins
- ❖ Complex Attack
- ❖ Indirect Fire and Direct Fire Attacks
- ❖ VBIED Attack
- ❖ Unexploded Ordnance (UXO)
- ❖ Missing Persons
- ❖ Kidnap and Ransom
- ❖ Mugging and Robbery
- ❖ Road Traffic Accident
- ❖ Civil Unrest
- ❖ Sabotage
- ❖ Demonstrations
- ❖ Loss of Sensitive and High-Value Materials
- ❖ Workplace Violence
- ❖ Threats, Intimidation, and Coercion
- ❖ Floods and Tidal Waves
- ❖ Earthquakes
- ❖ Pandemics
- ❖ Hurricanes
- ❖ Sandstorms
- ❖ Landslides
- ❖ Emergency Response Numbers

## INTRODUCTION

The Incident Management Plan (IMP) is a collection of instructions, guidelines, protocols, and procedures designed to meet a wide spectrum of potential risks faced by mobile laboratory operations. Mobile laboratories have a unique make-up: they are used in static locations for extended periods of time and yet could be relocated as needed. This makes all such facilities prone to static and in-transit threats. All mobile laboratories are therefore equipped with baseline security measures, including the following:

- Access Control Biometric Locks
- Reinforced Entry Doors
- Blast Film
- External CCTV for Intruder Detection
- Motion Sensors
- Vehicle Tracking Unit with Panic Button
- Redundant Communication Equipment
- External Perimeter Fencing: For Short-Term Locations

## SECURITY MANAGEMENT

Many operating environments may not have dedicated staff to oversee mobile lab security requirements. As such, staff working in the lab need to take ownership of risk and security management functions as well as incident and crises management roles. Creating a local incident management team within the staff available is a quick and simple process and should be focused on addressing the critical components of providing response in an organized and effective manner. Incident management teams will therefore always be composed of staff working within the mobile labs.

The security management team will include the following professional security members:

- Business Risk Department
- Country Director Business Risk
- Program Director Business Risk
- Incident and Crises Management Control Room
- Field Safety and Security Focal Person
- Security Field Officers (SFOs)

Notes:

- Other members assigned with each MBL will be identified in the Security Management Plan
- Before deployment of MBL, each team member will be assigned responsibility, and this will be indicated in the plans
- The IMT team based in the Islamabad Business Risk Department will manage all security functions in coordination with the field safety and security focal person and specialized security field officers deployed at each location

## GOALS AND OBJECTIVES

Provide a safe and productive operating environment for staff where risks are identified and either avoided or appropriately mitigated before they occur, or where emergencies are managed effectively and professionally.

## RISK MANAGEMENT

Lab staff should understand that threat perception varies, and tolerance levels may be different for individuals working in the field. Also, various levels of experience and knowledge may result in far different perceptions and tolerance levels within the same team. As such, a standardization of what is considered acceptable is required to best protect staff, operations, and assets. Levels of probability and impacts range from low, where the probability of a situation occurring is highly unlikely, to extreme, where staff should expect a risk to occur at some stage. The impacts associated with such events may be insignificant to extreme. By clearly defining probability and impact category levels, staff will quickly come to understand the evaluated probability occurring within the lifespan of an activity. Mobile labs must therefore be equipped with risk-rating tools for staff to understand the active threats and their associated risk.

The incident plan below outlines some of the most common threats expected for mobile lab staff. Guidelines provided should be amended based on each lab's operating environment:

### Vehicle Physical Security Breach

A physical security breach of a vehicle, whether in a remote, hostile, or permissive environment may pose a range of risks. Staff should consider the nature and intent of the breach, as well as the possible goals and motives of the intruders.

1. Stand up the incident management and crisis response teams,
2. Establish the nature of the breach (criminals, youth, activists, terrorists) and associated risk levels and types.
3. Elevate the alert status and post guards around the area.
4. Notify law enforcement organizations.
5. Determine where the breach occurred and secure it.
6. Perform a roll call of all staff; identify missing staff.
7. Close and secure the lab, and if necessary, move staff out.
8. Perform an inventory of all equipment, and documents, if appropriate.
9. Determine the consequences of the breach and begin mitigation to prevent future security breaches.
10. Conduct a sweep of the area for unauthorized intruders and devices.
11. Confirm whether intruders are still present; track and monitor movements, if possible.
12. Draft a complete detailed report of the breach.
13. Forward all information through the correct communication channels and update where needed.

### Small Arms Fire

Small arms fire is the use of rifles or handguns against a target, whether person, vehicle, or structure, presenting a personal and psychological risk to employees as well as secondary hazards if fired within areas with highly combustible materials. The caliber and velocity of the round as well as its composition and nature will determine the level of damage this form of threat may pose to staff or facilities. In the event of an incident, the following points should be addressed:

1. Stand up the incident management and crisis response teams.
2. Determine whether a hostile activity is underway:
  - a. Directly targeting individuals or the mobile lab.
  - b. Indirect gunfire within a broad beaten zone.

- c. Celebratory gunfire from festivals.
3. Determine whether the gunfire is effective. Is it hitting the intended targets, or is it indiscriminate?
4. Move staff to safe areas, if permissible.
5. Secure the laboratory, close all access points, and lock lab.
6. Instruct employees to take cover.
7. Alert external response groups, including police and dedicated emergency services, to intercede.
8. Stay covered until the situation is resolved.
9. Draft a complete detailed report of the incident.
10. Forward all information through the correct communication channels; update where needed.

### Hostage Situation

The speed and quality of decisions and actions taken during the initial stages of a hostage situation will likely have a significant influence on the outcome. The distinction between a hostage and kidnapping situation is that the location of the victim is known during a hostage situation. The nature of the operating environment will also determine the approach used. Hostage situations may involve disgruntled employees, personal disputes, criminals, or in the most extreme cases, activists or dissidents. Hostage negotiation is a specialist field, and managers should not enter discussions with the perpetrator. If an employee or contractor is being held hostage, the following immediate steps should be taken:

1. Stand up the incident management and crisis response teams.
2. Notify appropriate law enforcement, military, and government agencies for immediate assistance.
3. Establish the location of the incident, as well as details of perpetrator(s).
4. Secure the area, and if possible, contain the hostage situation to prevent escape or exposing other parties to follow-on risks.
5. Close off all vehicles exit routes to prevent the perpetrator and hostage vehicle escape (use unmanned vehicles if necessary to block routes).
6. Lock exit doors and routes to prevent escape by foot.
7. Cordon the area to prevent other employees being taken hostage; clear the area of all staff.
8. Send out notifications—email, phone, and text.
9. Seal access routes.
10. Establish a line of communication with the perpetrator, do try to NOT negotiate; inform the perpetrator that someone is on route who is authorized to make decisions.
11. Provide floor plans, maps, and other details to law enforcement upon arrival.
12. Establish an incident control point and safe access routes; notify external agencies and organize a reception to lead them into the location through a safe route.
13. Forward all information through the correct communication channels; update where needed.

### Domestic Terrorism and Special Interest Groups

Domestic terrorist or special interest groups may focus on MBL for a variety of reasons; typically, due to the nature of activity that falls within their area of interest. Domestic terror groups are generally nonviolent toward individuals (although can cause alarm and might engage in intimidation), but do often damage property and destroy materials, which can present a physical risk. Such groups leverage the media as a tool to promote their cause and should be managed with care so as not to further their agenda. In the event of an incident, the following points should be addressed:

1. Stand up the incident management and crisis response teams.
2. Secure the facility to prevent access to unauthorized personnel.
3. Alert the local police and request assistance.
4. Determine the immediate objectives of the group, to:
  - a. Steal information.

- b. Sabotage materials, facilities, or equipment.
- c. Elicit media attention.
- d. Instigate a physical or verbal response from employees or managers.
- e. Gain access to sensitive areas or stage a sit-in within offices or worksites.
- f. Barricade or impede access to areas.
- g. Intimidate, threaten, or harm employees.  
Plant harmful or hazardous materials.
- h. Conduct prank activities, disruptive in nature.
5. Do not physically touch any activists or their possessions, if possible.
6. Avoid inflammatory remarks or heated discussions.
7. Ask persons to leave a premises or worksite politely; inform them of any laws or regulations they are breaking.
8. Do not discuss company activities, policies, or plans.
9. Record the groups or individual's activities using cameras or CCTVs as part of investigation and legal response requirements.
10. Record their activities and note any risks posed to personnel, facilities, or materials.
11. Secure offices, laptops, and sensitive information if an intruder has been reported.
12. Engage other elements of the IMP if specific threats are presented (assault, intimidation, fire, damage, espionage, etc.).
13. Send regular situation reports to the crisis response team.

#### Site Occupation and Sit-Ins Incident

Site occupation or sit-ins may occur for a variety of reasons. Domestic terror or special interest groups may seek to stage a public protest. Site occupation or sit-ins may be peacefully conducted or may be violent. Durations of occupancy may be shorter may be for extended periods of time, especially if personnel cannot be evicted safely. In the event of an incident, the following points should be addressed:

1. Stand up the incident management and crisis response teams.
2. Secure the facility to prevent access to unauthorized personnel.
3. Alert the local police and request assistance.
4. Determine the immediate objectives of the group, to:
  - a. Steal information.
  - b. Sabotage materials, facilities, or equipment.
  - c. Elicit media attention.
  - d. Instigate a physical or verbal response from employees or managers.
  - e. Gain access to sensitive areas or stage a sit-in within offices or worksites.
  - f. Barricade or impede access to areas.
  - g. Intimidate, threaten, or harm employees.
  - h. Plant harmful or hazardous materials.
  - i. Conduct prank activities, disruptive in nature.
5. Do not physically touch any activists or their possessions, if possible.
6. Avoid inflammatory remarks or heated discussions.
7. Ask persons to leave a premises or worksite politely; inform them of any laws or regulations they are breaking.
8. Do not discuss company activities, policies, or plans.
9. Record the groups or individual's activities using cameras or CCTVs as part of investigation and legal response requirements.
10. Record their activities and note any risks posed to personnel, facilities, or materials.
11. Secure offices, laptops, and sensitive information if an intruder has been reported.
12. Engage other elements of the IMP if specific threats are presented (assault, intimidation, fire, damage, espionage, etc.).



13. Send regular situation reports to the crisis response team.

### Complex Attack

A complex attack is when a hostile person or group uses several forms of attack against a target concurrently. The complex attack typically aims to kill or injure as many people as possible, significantly damage mobile lab, or enable instigators to affect a kidnap. Such attacks usually are more thoroughly planned than other forms of risk and are typically aimed at a specific target rather than being opportunistic due to the complexity of planning required and the resources required. Effective risk mitigation and security planning will form the basis for avoiding complex attacks. In the event of an incident, the following points should be addressed:

1. Stand up the incident management and crisis response teams.
2. Mobilize all security staff and implement security response protocols.
3. Notify employees to move to safe zones if possible.
4. Lock down access control points and restrict unauthorized movements.
5. Notify supporting police agencies.
6. Determine the size and composition of the aggressor group; relay to the security response staff.
7. Implement other aspects of the IMP as they relate to the incident.
8. Other instructions.

Provide a post-incident report when the crisis is over.

### Indirect Fire and Direct Fire Attacks

An indirect fire attack is one in which a device such as a rocket or mortar round is fired by launching the round into the air with the aim of it landing on or near its target. On striking the ground the round will detonate, creating a blast wave and throwing shrapnel in all directions, or may not detonate and result in unexploded ordnance hazards. There may be no warning of an incoming round, and if a round explodes near laboratory staff, it should be assumed that several more rounds may be inbound. In the event of an incident occurring, the following points should be addressed:

1. Stand up the incident management and crisis response teams.
2. Sound the alarm to notify staff of incoming risks (alarm types of sirens, texts, phones, shouting).
3. Move staff to take cover, if safe to do so.
4. Alert staff outside of the affected area who may be moving toward the risk area.
5. Conduct a roll call of all staff, account for missing persons.
6. Alert supporting agencies, police or other.
7. Close the laboratory secure access control points; prepare for secondary attacks.
8. On completion, manage casualties and damages.
9. Conduct a UXO sweep before allowing staff to resume duties.
10. Determine the damages in terms of:
  - a. Indirect fire (IDF) attack damages to lab and resulting hazards.
  - b. Unexploded ordnance (UXO) damages, fires, and explosions.
  - c. Follow-on small arms fire or complex attacks, and IDF fragmentation hazards.
  - d. Casualty management and evacuation procedures.

### VBIED Attack

A vehicle-borne improvised explosive device (VBIED) will either be in the form of a static vehicle, set on a timer, tilt mechanism, or remotely detonated. Or it will be in the form of a mobile/static suicide bomber. SOPs should be in place to limit the opportunities for unauthorized vehicles containing explosives to enter a secured area.

This will include physical measures (barriers, gates, guards) and policies and procedures. In the event of an incident occurring, the following points should be addressed:

1. Stand up the incident management and crisis response teams.
2. Take shelter (lay down, move behind, move away). Refer to explosive hazard distances diagram for details.
3. Notify emergency services immediately.
4. Establish a casualty management point if an explosion has occurred.
5. Assist casualties and walking wounded—provide casualty reports as per the communications plan.
6. Establish an incident control point to coordinate responses and meet external response groups; notify responding agencies of the location and of safe routes intimation.
7. Confirm there are no “secondary” devices; conduct a security sweep.
8. Implement the six Cs:
  - a. **Confirm** the presence of the suspect device. This should be a one-person task (if appropriate) and needs to be done from a distance whenever possible. Maximum use should be made of hard cover and spotting equipment through such means as binoculars or scopes.
  - b. **Clear** the area around the device of all staff, working from the device outwards, to 300m. Maximum use should be made of hard cover, such as buildings. No one should be in clear sight of the threat area.
  - c. **Cordon** the 300m danger area and set up an incident control point (ICP) for follow on agencies to meet at. Staff who are being cleared from the area should be checked at random to deter additional threats.
  - d. **Control** the area inside the cordon to ensure only authorized access is achieved. Only emergency services should be allowed to breach the cordon through the control point. Any breaches of the cordon should be reported immediately to the IRT Commander.
  - e. **Check** all staff stationed on the cordon should check their immediate area for secondary devices and hazards. Any suspicious items should be reported to the situation commander and their position marked.
  - f. **Coordinate** activities between mobile lab and emergency responders. Effective coordination is critical for the safe resolution of the situation.
9. Send out security alerts to notify staff to avoid the area if traveling—prevent persons from entering the danger zone.
10. Notify medical facilities and support agencies.
11. Carry out a roll call of all employees and staff; locate missing persons.
12. Begin a running log of events as they occur, recording activities.
13. Do not divulge the names of casualties until their next of kin has been notified.
14. Provide a serious incident report as soon as possible.
15. Cordon off the site of a detonation—this is relevant for any forensic investigations, as well as mitigating the threat from any secondary devices or unexploded ordnance.

### Unexploded Ordnance IED or Suspect Package

The mishandling of a suspect package or unexploded ordnance can result in injury, death, and the loss of forensic evidence. Such materials may be left in small bags, might be disguised as rubbish bags or in coke cans, might be portions of partially detonated munitions, or might be booby trapped materials. At all times, incident managers should consider the safety of the persons involved in the operation, the integrity of the evidence, the requirement not to touch the suspect package or item, the need to clear the area quickly and safely, and the need to pass on

information so that specialist responders can deal with the situation. Should a suspect package or unexploded ordnance situation occur, the following immediate steps should be taken:

1. Stand up the incident management and crisis response teams.
2. Initiate a site evacuation plan if required. Consider threats posed by moving staff, ensure escape routes are not exposed to UXO or suspect package risks. Determine whether it is safer to have staff remain where they are or move.
3. Do not use radios or mobile phones near the device.
4. Confirm: Confirm it is an explosive package, do not touch, and remember the 5 Ws:
  - a. **What** have you found: get a description, size, shape color, wires visible? Take photos if possible and do not approach or touch.
  - b. **Where** was it found: 10 figure grid reference or other reference point.
  - c. **When** was it found: time and date?
  - d. **Why** are you there.
  - e. **Whether** it has been moved or touched.
5. Clear the area to ensure the safety of staff; no one should be in line-of-sight of the package. The following elements should be considered:
  - a. Radio transmissions only at a safe distance, handheld; vehicle fitted.
  - b. Mark the route to the UXO or suspect package.
  - c. Establish an incident control point to notify external agencies of location and safe route in.
  - d. Wedge open doors (allow clear access and exit for staff).
  - e. Evacuate staff to safe locations; conduct musters to identify missing persons.
6. **Cordon** until emergency services arrive to assume control:
  - a. Establish correct cordon distances (see table).
  - b. Ensure all staff, including security, are out of line of sight of the package or material.
  - c. Ensure that staff are not at risk from secondary hazards.
  - d. Ensure staff are behind hard cover, if possible (concrete walls).
  - e. Ensure staff are not observing the incident from behind windows (blast effects).
  - f. Ensure staff are upwind if chemical or other such hazards are present.
7. **Control** the situation until relieved or the emergency services arrive.
  - a. Control the scene and area.
  - b. Establish safe routes and control points.
  - c. Ensure all persons are not in line-of-sight of the materials (300–500m).
  - d. Ensure that the control room is aware of any action you take; be accurate with your information.
8. **Check** the areas of other threats as well as evidence.
  - a. Check for secondary hazards.
  - b. Ensure the location is protected for police investigations.
  - c. Save evidence if any on site.
  - d. Secure the area.
  - e. Consider other potential and present hazards.
9. Assess any damage to the site after an explosion. Also implement the casualty response procedures.
10. Forward all information through the correct communication channels, update where necessary.

Safety Table for Unexploded Ordnance and Suspect Packages

Threat Description	Explosive Capacity (TNT Equivalent)	Threat Distances	Outdoor Evacuation Distances
Pipe Bomb	5 lb or 2.3 kg	70 ft or 21 m	850 ft or 259 m
Briefcase/suitcase bomb	50 lb or 2 kg	150 ft or 26 m	1,850 ft or 564 m
Small car bomb	500 lb or 227 kg	320 ft or 98 m	1,500 ft or 475 m
Large car bomb	1,000 lb or 454 kg	400 ft or 122 m	1,750 ft or 534 m
Passenger van bomb	4,000 lb or 1,814 kg	600 ft or 195 m	1,750 ft or 838 m
Small moving van bomb	10,000 lb or 4,536 kg	860 ft or 263 m	3,750 ft or 1,143 m
Moving truck bomb	30,000 lb or 13,608 kg	1,240 ft or 375 m	6,500 ft or 1,982 m
Semi-trailer bomb	60,000 lb or 27,216 kg	1,500 ft or 457 m	7,000 ft or 2,134 m

### Missing Persons

In high-risk locations a failure to report in or communicate with manners may result in staff being reported and considered “missing” within a short timeframe. Within typical operating environments it is common that the term “missing” is applied only after the person has been out of contact for more than 24 hours (36 hours in a low-risk area). The following steps should be taken:

1. Stand up the incident management and crisis response teams.
2. SSFP is to establish facts with the last person to be in contact with the missing person.
3. Inform the appropriate law enforcement or military agencies.
4. Check with local hospitals to see if the person has been admitted.
5. Check with local police stations to see whether the person has been arrested or reported injured.
6. Ascertain the last known whereabouts of the person and who if anyone they were with.
7. Check personnel records to see if the person has a medical condition, or a history of losing consciousness as well as any medical risks they might face.
8. Contact all possible locations (business and personal) where the person may have visited, or where they may now be.
9. Determine whether security teams or personnel can search areas or locations where the person might be.
10. Liaise with the person’s family through an appointed manager.

### Kidnap and Ransom (K&R)

Kidnapping is a specialist area and must be treated with the utmost professionalism and sensitivity. The distinction between a hostage and kidnapping situation is that the location of the victim is not known during a kidnapping situation. In certain environments the ability to recover kidnapped persons might be possible using western military force support to cordon or search areas, if the proper incident management policies, agreements, and standard operating procedures are in place. In other environments, it will be the remit of solely a K&R team to recover kidnapped persons. In the event of a kidnapping the following (initial) steps should be taken to ensure the safety of the victim:

1. Stand up the incident management and crisis response teams.
2. Liaise with nearby police or military commander, if authorized.
3. Be sure that a kidnapping has indeed occurred; explore all possible explanations for a missing person (see missing person guidelines).
4. Confirm where the victim was last seen, and with whom—get a full statement of events, as well as what the victim was wearing.

5. Determine whether the victim has any medical conditions and the state of their mental health.
6. Start a log of events and update it as events transpire.
7. Alert expert consultants and negotiators (if sanctioned).
8. Notify the victim's family (if sanctioned).
9. Limit information given to the media for the wellbeing of the victim.
10. Choose a telephone to be used when talking to kidnappers and attach a recording device if possible.
11. Retrieve personal file of victim so that "proof of life" questions can be verified.
12. Do not indicate to kidnappers that police have been notified (if appropriate).
13. Promise nothing but be conciliatory.
14. Allow the experts to do their job once they arrive on scene.
15. Take notes or record details such as voice, age, timbre, race, gender of kidnappers.
16. Take statements from any witnesses who may have witnessed the event, description of kidnappers, vehicles, and other details.
17. Place all evidence in plastic bags; handle corners only to avoid damaging fingerprints.
18. Forward all information through the correct communication channels; update as needed.

### Mugging or Robbery

Robbery or mugging is a risk faced within any part of the country. Staff should avoid demonstrating their wealth, should carry limited cash or valuable items, and should always seek to remain in public and well-lit spaces. If a person is robbed or mugged, they are generally advised not be aggressive, but hand over their money and possessions without resistance, remaining calm so as not to excite the robber. Typically, robberies are motivated by crime, rather than a personal grudge, and most criminals will depart after being given money or valuable items. In the event of an incident, the following points should be addressed:

1. Stand up the incident management and crisis response teams.
2. Determine whether anyone was injured, physically or psychologically.
3. Seek medical assistance if injuries occurred and counseling, if appropriate.
4. Determine what was stolen and its value to the individual as well as the Lab Ops.
5. Inform the police, providing:
  - a. Date, time, and location of occurrence.
  - b. Injuries resulting from the event.
  - c. Items stolen.
  - d. Description of the assailant.
  - e. Any history associated with the area or individual of assaults and robberies.
6. Review the security measures or advisory briefing for the area in which the crime occurred.
7. Determine whether risks are posed to staff within and outside of the laboratory.

### Road Traffic Accidents

Road Traffic Accidents can be relatively mundane events within some environments, or quickly escalate into significant events in others:

1. Stand up the incident management and crisis response teams.
2. Determine the extent of injuries of those involved (if any).
3. Find out where injured parties were taken and if the injuries warranted hospitalization.
4. Determine if local authorities or staff are involved, and if the occupants of the mobile lab are being charged with a crime.
5. Establish the location and status of mobile lab, arrange for the retrieval of the mobile lab and any property if it is immobile.

6. Begin to record information within the record of events log.
7. Liaise with local police authorities to seek their support (if appropriate).
8. Be sure to fill out the Driver Accident Report Form completely and accurately.
9. Forward all information through the correct communication channels, update where necessary.

## Civil Unrest

Civil unrest may be isolated and short-term events or be widespread and long-lasting crisis situations. Civil unrest can involve the direct or indirect targeting of staff, resources and assets, as well as transiting staff and materials. Crime and social disorder are often associated with such situations. Staff may also be exposed to risks associated with police responses if caught within a crowd or riot event. If a civil unrest situation occurs the following immediate steps should be taken:

1. Alert security staff—appropriate security response measures should be taken, enhancing security alert states and measures.
2. Alert supporting police and law enforcement agencies—request advice and support.
3. Gather all available intelligence on the situation.
4. Determine the nature, tempo, scope and impacts of the civil unrest situation.
5. Determine which resources are most at risk.
6. Secure lab, materials and resources.
7. Send local employees and work forces home if safe to do so.
8. Move non security staff to safe areas, account for missing staff.
9. Move staff away from crowds and out of sight if necessary. Staff are to stay away from windows or other apertures and stay behind solid structures.
10. Ensure staff are removed from combustible or flammable materials.
11. Consider the implementation of an evacuation plan if required, or appropriate.
12. Forward all information through the correct communication channels; update as needed.

## Sabotage

The sabotage of a facility or equipment can be through common vandalism damaging or making resources inoperable or faulty or may be through focused and well-planned activities by organized crime, special interest groups or terrorists. Sabotage may place staff at risk, may disrupt operations or may result in other secondary risk effects. In the event of an incident occurring the following points should be addressed:

1. Lock down the lab— alert staff and move employees to safe area if necessary.
2. Mobilize security staff to secure access points—all area movements to stop until response measures are completed.
3. Conduct security sweeps and searches to locate any additional acts of sabotage, as well as search for saboteurs.
4. Determine what has been sabotaged:
  - a. Equipment
  - b. Materials
  - c. Systems
  - d. Technology and Communications
5. Are the saboteurs still on site—can they be detained by security or police agencies.
6. Are the saboteurs violent, are they armed... how will they respond if apprehended – what risks are associated with the individuals themselves.
7. Determine what risks are connected to the act:
  - a. Explosive.
  - b. Failure.

- c. Disruptive.
  - d. Toxic.
  - e. Structural.
  - f. Information.
8. What risks are presented to staff directly, or because of secondary hazards.
  9. Document and photograph sabotaged materials, assets or structures.

### Demonstrations.

Many groups will use public demonstrations to gain media exposure, as well as impede business activities. Demonstrations may be singular events; lasting hours, or may be protracted, lasting days to months and evolving into site occupancy. Demonstrations are typically non-violent and involve chanting, banners and costumes. Demonstrations may also involve the symbolic burning of items, or the leaving of obstructive or unpleasant items such as manure and tree stumps. In the most extreme cases demonstrations may lead to an escalation in violence and may turn into riots. In the event of an incident occurring the following points should be addressed:

1. Establish the temperament of the demonstration; is it violent, disruption, intimidating, peaceful...
2. Establish the agenda and objectives of the individuals or groups—who are they and what do they want to accomplish; and how.
3. What risks are presented to staff directly, or because of secondary hazards.
4. Lock down the mobile lab – alert staff and move employees to safe areas.
5. Raise the alert status and security posture—mobilize security staff, closing access control points.
6. Mobilize security staff to secure access points and high-value areas—all area movements to stop until response measures are completed.
7. Conduct security sweeps and searches to locate any acts of sabotage, as well as search for demonstrators.
8. Alert law enforcement agencies manage demonstrators—indicate whether any unlawful acts have been conducted and the temperament of the demonstration.
9. Cordon the affected area or resources to contain, where possible and appropriate, the demonstration.
10. Document and photograph the demonstration in case an investigation or legal action is required post event.

### Loss of Sensitive or High-Value Materials

The loss of sensitive or high-value materials, equipment or information can have significant operational implications. Staff should identify which materials, resources or equipment might be considered sensitive or of high value and attribute measures by which to protect such items. Risks may include espionage, loss, theft, damage or destruction. In the event of an incident occurring the following points should be addressed:

1. Establish the nature and details of the material or item: determine how it was lost.
2. Determine the impact of the loss or damage to sensitive or high-value materials; both direct and peripheral.
3. Confirm the last location and owner responsible for the material or item.
4. Gain written reports from the person to whom the item was assigned.
5. Confirm whether the item was destroyed or was left intact at the scene or work site.
6. Liaise with appropriate authorities to recover the item or confirm destruction.
7. Take appropriate actions to mitigate the risks associated with the loss of the item, especially for communications or intelligence sensitive materials.
8. Confirm standard operating procedures were followed—provide a post-incident report.

## Workplace Violence

Workplace violence can have significant impacts on staff safety and operational productivity, as well as result in serious legal and liability issues. Workplace violence can quickly reduce morale, increase absenteeism, elevate stress, create retention and recruiting issues, as well as bring negative publicity and reputational challenges. Risks can range from verbal abuse or inferred threats to simple assaults, aggravated assaults, robberies, thefts, hostage taking, hijackings, and rapes and sexual assaults to shootings and fatalities. Should an incident occur, address the following points:

1. Determine who is at risk, move them out of confrontational situations or the risk area.
2. Determine what risks are present:
  - a. Is the aggressor physically or verbally violent?
  - b. Does the aggressor have a history for violence?
  - c. Is the aggressor armed in any way?
3. Mobilize local security and or police to intercede immediately restraining the provocateur if necessary (as a last resort).
4. Attempt to diffuse the situation if safe and appropriate.
  - a. Always work with others rather than in isolation.
  - b. Avoid aggressive postures or inferences.
  - c. Suggest the aggressive comes back later to discuss with senior management to diffuse the situation and enable police to respond.
5. Avoid confrontational discussions, placate the aggressor while police or security staff respond if possible and appropriate.
6. If others are at risk, clear the area if required.
7. Provide a post-incident report as soon as possible.

## Threats, Intimidation and Coercion

Coercion is the practice of compelling a person to behave in an involuntary manner either through action or inaction, using threats, intimidation, or some other form of pressure or force. Extortion occurs when a person either unlawfully obtains money, property, or services from a person, entity, or institution through coercion or intimidation, or threatens a person, entity, or institution with physical or reputational harm unless he or she is paid money or property. Should an incident occur, the following points should be addressed:

1. Establish which individuals or groups are at risk.
2. Establish who the perpetrator or group is that is threatening the individual.
3. Establish their agenda, motivation and goals; determine the implications for staff, activities, and facilities.
4. Establish the nature and impacts of the risk, as well as the probability of occurrence:
  - a. Is it an empty threat?
  - b. Is it a real threat?
5. Take precautions to safeguard individuals, groups, or facilities while police and other response groups are mobilized.
6. Inform the police, providing as much detail as possible.
7. Collect any evidence of the threats made for investigations and possible prosecution.
8. Increase the security and safety posture in locations at risk.

## Floods and Tidal Waves

Flood effects may be limited to a local area, affecting low-laying areas or adjacent to a river, or may be widespread affecting entire river basins. Floods may occur within a matter of minutes (flash floods) or may develop slowly over a period of days. Flash floods often have a dangerous wall of water that carries rocks, mud, and other debris and can sweep away buildings, vehicles, and other structures in its path, occurring with little sign of the rainfall



that initiated the event. Tsunamis, also known as seismic sea waves or tidal waves, result from a series of enormous waves created by an underwater disturbance such as an earthquake, landslide, or volcanic eruption, occurring with little if any warning. A tsunami can move hundreds of miles per hour in the open ocean and strike land with waves as high as 100 feet or more. In the event of an incident occurring, the following points should be addressed:

1. Determine the location of the risk, the direction, and the speed of travel to evaluate the likely affected risk area.
2. Move staff to high ground if possible. If remaining in vehicle, then utilities should be switched off and sensitive materials moved to the higher levels.
3. Avoid areas that might channel flood waters—low-lying ground, wadis, riverbeds, valleys, etc.
4. If time permits, use water barriers (such as sandbags) to seal door-jams, cracks, windows, etc. to stop or slow water entering MBL.
5. Place indicators for emergency responders that staff are trapped within MBL, indicating number and any support needed.
6. Monitor radio stations to track the event and its possible effects.
7. Avoid movement through moving water—it can sweep staff off their feet and disguise hidden hazards.
8. Avoid moving through flooded regions due to contamination and health hazards.
9. Do not drive through a flooded area—it will disguise holes; hazards and two feet of moving water can sweep vehicles downstream.
10. Drink only bottled or stored water—utilities may have been contaminated.
11. Be aware of secondary hazards—pipelines (gas, water, sewer) may have been ruptured, power cables may have electrified water, and crime and health hazards may increase.
12. Implement other aspects of the IMP as appropriate.

## Earthquakes

Earthquakes are a result of tectonic plate movements that cause the ground to shift or vibrate, bringing structural damages that can cause fires, gas leaks, collapsed buildings, flooding caused by ruptured pipes, damage to bridges and other structures, and the shattering of fragile or glass structures. Earthquakes can consist of a sequence of foreshocks and aftershocks. Commonly, public utilities and communications are disrupted by severe earthquakes, as are emergency services. In the event of an incident occurring, the following points should be addressed:

1. Move staff to a prearranged safe location. If no such facility is available, staff should seek refuge under sturdy tables or doorframes.
2. Where possible, gas supplies should be turned off and open flames should be quenched.
3. Before the earthquake occurring, staff should seek to secure all loose possessions, especially large, heavy, and breakable items.
4. During the earthquake, staff should drop to the ground and take cover until the shaking stops, covering their heads with their arms, and positioned away from glass, windows, outside doors, and walls.
5. If outdoors, staff should be advised to stay outside and move away from buildings, streetlights, and utility wires until the shaking ceases.
6. If in a moving vehicle at the time of the earthquake, staff should stop as quickly as safety permits and remain within the vehicle. Vehicles should avoid stopping near or under buildings, trees, overpasses, and utility wires.
7. After an earthquake, aftershocks may occur, as well as secondary hazards such as fires, floods, explosions, or tsunamis. Staff should be aware that gas leaks might result in fires.

8. Should staff be trapped within collapsed buildings, they should not light a match or move about and disturb any dust or debris; rather, they should cover their mouths with a handkerchief or clothing and tap on a pipe to assist rescuers in locating them.
9. Account for missing staff, manage injuries, and report as per other IMP instructions.
10. Other elements of the IMP should be instigated as appropriate.

## Pandemics

A disease outbreak or pandemic is the occurrence of incidences of disease more than what would normally be expected within a defined community, geographical area, or season. An outbreak may occur in a restricted geographical area or may extend over several countries. The risk period may be short, lasting several days or weeks, or may be protracted, lasting months or years. A particular case of a communicable disease long absent from a population or caused by an agent (e.g., bacterium or virus) not previously recognized in that community or area, or the emergence of a previously unknown disease, may also constitute an outbreak and should be reported and investigated. In the event of an incident occurring, the following points should be addressed:

1. Determine the affected area and nature of the pandemic. Are MBL staff or operations within or near an affected area? Have staff just returned from the affected area?
2. Determine the response actions being taken by government or other groups. Are they effective?
3. Determine whether anyone within the staff has been infected.
4. Evaluate whether it is safer to evacuate staff or remain in place.
5. How long will people be permitted to leave the area by local authorities?
6. Can the local authorities manage the situation? Do they have the capacity and expertise?
7. Are resources sufficient to remain in place, notably, food and water?
8. Can vaccines and medicines be mobilized to support management of the pandemic?
9. Are there other threats that might result from the pandemic, such as civil disorder, utility disruptions, and essential material deliveries?
10. Should the staff be sent home? What instructions of support can be offered?
11. Evaluate what resources are required to move MBL staff to a safe location.

## Hurricanes

A hurricane is a type of tropical cyclone, which is a generic term for a low-pressure system that generally forms in the tropics. It is defined as an intense tropical weather system of strong thunderstorms with a well-defined surface circulation and maximum sustained winds of 74 mph or higher. In the event of an incident, the following points should be addressed:

1. The location, direction, and speed of travel of the storm should be determined to evaluate which areas are most susceptible to risk (although changes in directions can occur).
2. If time permits, MBL windows should be boarded up as an emergency solution if storm windows or shutters have not been fitted.
3. Staff should be moved to nominated safe areas.
4. Staff should avoid windows, skylights, and glass doors, as debris and fierce winds may shatter such structures.
5. Staff should not leave a safe location when in the eye of the storm but must wait until the storm has passed over; since there will be a brief period of calm followed by a rapid increase in wind speed from the opposite direction.
6. In case of flooding, electricity should be turned off at the main breaker. If MBL loses power, all electronic equipment should be turned off, such as the air conditioner, to reduce damage.
7. Staff should be advised not to touch fallen or low-hanging wires and to stay away from puddles with wires in or near them if leaving buildings.

8. Monitoring of radio stations will provide information on the storm's passage, as well as emergency response measures being taken.
9. Other aspects of the IMP should be carried out as appropriate (flooding, landslides, pandemics, etc.).

### Sandstorms

Sandstorms are recognizable as a large cloud traveling over the ground, occurring frequently in most deserts. Some sandstorms occur for only a matter of hours; some can blow constantly for up to a few days at a time. In the event of an incident occurring, the following points should be addressed:

1. The location, direction, and speed of traveling sandstorms should be determined to evaluate which areas will be most likely affected.
2. Before a sandstorm occurring, windows, vents, and skylights should be closed to prevent dust from entering facilities.
3. Vehicles should be turned off (unless especially prepared) to avoid damaging the engine.
4. If staff are required to operate outside, they should be advised to lubricate their nostrils with petroleum jelly (if available) to prevent the mucus membranes drying out.
5. Staff should be instructed to tie a cloth over their nose and mouth and wear goggles to protect their vision when exposed to the sandstorm.
6. Staff should also be instructed to remove contact lenses, tuck in clothes (tops into pants, pants into socks) to prevent burns from the sand, wearing long sleeves and trousers.
7. Visibility may become extremely limited, and groups working outdoors should be attached by ropes to prevent staff from become disorientated and lost.
8. Staff should be mustered within a defined space and missing persons accounted for.
9. Other elements of the IMP should be implemented as appropriate.

### Landslides

A landslide is a phenomenon that includes a wide range of ground movement, such as rock falls, deep failure of slopes, and shallow debris flows. Landslides may also be caused following heavy rains or earthquakes. In the event of an incident, the following points should be addressed:

1. Staff should be advised to avoid steep slopes, especially close to mountain edges, near drainage ways, or natural erosion valleys.
2. During a landslide, staff should be advised to stay alert and awake, since many debris flow fatalities occur when people are sleeping.
3. If MBL staff are in areas susceptible to landslides and debris flows, consideration should be given to departing the area as the first indicators of a possible landslide occur.
4. After a landslide, staff should stay away from the slide area, following directions from local news or television stations.
5. Additional hazards include flooding, damaged roadways, and public utilities, including broken gas pipes.
6. Staff should be mustered, and missing staff must be accounted for.
7. Other elements of the IMP should be instigated as appropriate.

## Emergency Response Numbers

Response Category	Primary Number	Alternative Number
Police		
Rangers		
Civil Defense		
Bomb Disposal		
Ambulance Services		
Fire Brigade		

Please keep the table up to date and add new numbers as required.

## Annex 3: Incident Reporting Form

Location name:	
Mobile lab ID:	
Date of report:	
Reporter name and position:	
Reporter telephone:	
Reporter email:	
Reporter mailing address:	
Date of incident:	
Time of incident:	
Name of principal investigator:	
What was the <b>nature</b> of the incident?	<ul style="list-style-type: none"> <li>↑ Personnel exposure</li> <li>↑ Spill</li> <li>↑ Loss of containment</li> <li>↑ Loss of PPE</li> <li>↑ Failure to obtain administration approval</li> <li>↑ Failure to follow approved containment conditions</li> <li>↑ Other—please describe:</li> </ul>

Did the proper approval was taken for this work	↑YES ↑NO If yes, on what date?
If yes, please provide:	Approval date:
	Approved biosafety level(s) for the work:
	Additional approval requirements (if any):
<p>Please provide a narrative of the incident, including a timeline of events. The incident should be described in sufficient detail to allow for an understanding of the nature and consequences of the incident. <b>Include the following information as applicable.</b></p> <p>A description of:</p> <ul style="list-style-type: none"> <li>• The incident/violation location (e.g., laboratory biosafety level, non-laboratory space)</li> <li>• Who was involved in the incident/violation, including others present at the incident location? <b>Note: please do not identify individuals by name. Provide only gender and position titles (e.g., lab manager, lab technician, mobile facility maintenance worker)</b></li> <li>• Actions taken immediately after the incident/violation, and by whom, to limit any health or environmental consequences of the event</li> <li>• The training received by the individual(s) involved and the date(s) the training was conducted</li> <li>• The institutional or laboratory standard operating procedures for the work and whether there was any deviation from these SOPs at the time of the incident/violation</li> <li>• The personal protective equipment in use at the time of the incident/violation</li> <li>• The occupational health requirements for laboratory personnel involved in the research</li> <li>• Any medical advice/treatment/surveillance provided or recommended after the incident</li> <li>• Any injury or illness associated with the incident</li> <li>• Medical surveillance results (if not available at the time of initial report, please indicate when results will be available)</li> <li>• Equipment failures</li> </ul> <p>DESCRIPTION OF INCIDENT: (use additional space as needed)</p>	

DESCRIPTION OF INCIDENT: (continued)	
Has the administration reviewed this incident?	↑YES ↑NO  If yes, please provide a copy the minutes of the IBC meeting in which the incident was reviewed.
Has a root cause for this incident been identified?	↑YES ↑NO  If yes, please describe:
Describe measures taken by the institution to mitigate any problems identified. For measures identified but not yet taken, please include a timeline for their implementation: (use additional space as needed)	

- **Please provide copies of any documents referenced in this report.**

**Signatures:**

**Reporting Person**





## Annex 4: Serious Incident Reporting template

### INCIDENT MANAGEMENT PLAN INFORMATION CAPTURE REPORTS

#### Serious Incident Report Incident Management Data Call

##### Lab Information

<b>SSFP Name:</b>		<b>Incident Date:</b>	
<b>Lab Location:</b>		<b>Report No:</b>	Initial/Interim/Final
<b>GPS:</b>		<b>Report Code:</b>	<i>I.E SIR-Rep</i>
		<b>Lab Code:</b>	
<b>Restriction Level:</b>		<b>Distribution Code:</b>	

##### Reporting Authority

Appointment	Name	Telephone	Email

##### Information Data-Call

Ref	Report Factor	Report Facts
1	Name:	
2	Location:	
3	Personnel Involved:	
4	Injuries (nature and names):	
5	Fatalities (names):	
6	General description of incident:	
7	When did it occur:	

**INCIDENT MANAGEMENT PLAN  
INFORMATION CAPTURE REPORTS**

8	Is the event ongoing, or complete:
9	What risks remain:
10	What assistance is required:
11	What assistance has been called upon:
12	Local government involvement:
13	Military or LEA involvement:
14	What local crisis management actions have been taken, what policies implemented – <i>what are you doing:</i>
15	Photos and map references of the incident:
16	Damages to facilities or assets:
17	What assistance is required:
18	Other information:

It is useful to catalogue and distribute measures which have been tried and have either failed or succeeded during a crisis situation in order to avoid duplication, demonstrate efforts being taken to a wider audience, as well as illustrate the degree of focus being paid towards resolving an issue. It also provides a failsafe to ensure no options are accidentally overlooked. A common failing found within response measures will be for the crisis management team, to not mention failed efforts, rather focusing on successful approaches.

Problem	Approach	Success / Failure	Explain Result	Led By	When Tried

## Annex 5: Event Management

The designated national and provincial OSROs of the mobile BSL-2 laboratory will notify the head of laboratory services in each province, office of the director general health services, and chief public health laboratory at NIH, Islamabad. The OSRO will also investigate reported incidents and provide a written critique of the incident.

### Physical Deterrents and Damages

In case of a physical accident on road, or any technical fault in the operations of the vehicle, the driver and/or other laboratory staff on board will immediately notify emergency first responders, local security forces, and the designated OSRO for personnel and lab safety and security.

#### Road Traffic Accident

Road traffic accidents can be relatively mundane events within some environments, or quickly escalate into significant events in others:

1. Establish the location and status of the mobile lab, arrange for the retrieval of the mobile lab and any property if it is immobile.
2. Liaise with local police authorities to seek their support.
3. Determine the extent of injuries of those involved (if any).
4. Find out if and where injured staff were taken; and if the injuries warranted hospitalization. Post-exposure medical protocols are part of SOPs for Avoiding Occupational Hazards Occupational Health Support Service Elements presented in Annex 7.
5. Be sure to fill out the Driver Accident Report Form completely and accurately.
6. Determine if local authorities or personnel are involved and if the occupants of the mobile lab are being charged with a crime.

### Disorderly Conduct, Violent Altercations, Fights, Riots

All labs will have emergency responders' numbers affixed next to the entry door. Lab staff will be provided a security briefing before any movement. As mentioned above, all movement plans are well coordinated with the local authorities/law enforcement agencies who will nominate their local representatives for emergency contact.

In case of an imminent insurgent attack, or of a violent incident aboard the laboratory, stop the activity, follow rapid inactivation protocols (Annex 8), and alert the OSRO, district health Officer to notify the nearest law enforcement agency. Security assessments will be carried out by provincial lab focal persons in coordination with district administration/LEAs. Based on this assessment, the lab staff will be advised to follow the response measures according to the geographical context. Also, security gears will be provided.

Workplace violence can have significant impacts on personnel safety and operational productivity, as well as result in serious legal and liability issues. Workplace violence can quickly reduce morale, increase absenteeism, stress, retention and recruiting issues, as well as bring negative publicity and reputational challenges. Risks can range from verbal abuse or inferred threats to simple assaults, aggravated assaults, robberies, thefts, hostage taking, hijackings and rapes. and sexual assaults to shootings and fatalities. In the event of an incident, the following points should be addressed:

- Determine who is at risk; move them out of confrontational situations or the risk area.
- Determine what risks are present:
  - a. Is the aggressor physically or verbally violent?
  - b. Does the aggressor have a history for violence?

- c. Is the aggressor armed in any way?
- Mobilize local security and/or police to intercede immediately restraining the provocateur, if needed (as a last resort)
- Attempt to diffuse the situation if safe and appropriate
- Always work with others rather than in isolation; the general rule for using/operating this lab should be that the work is conducted in pairs
  - a. Avoid aggressive postures or inferences.
  - b. Suggest the aggressor come back later to discuss with senior management, diffuse the situation, and enable police to respond.
- Avoid confrontational discussions; placate the aggressor while police or security personnel respond if possible and appropriate
- Are others at risk, clear the area if required. Law enforcement will determine the risks posed to others and determine if the surrounding area should be cleared. Security personnel will assist in this task
- Provide a post-incident report as soon as possible

## Sabotage

The sabotage of a facility or equipment can be through common vandalism damaging or making resources inoperable or faulty or may be through focused and well-planned activities by organized crime, special interest groups or terrorists. Before use or movement, laboratory staff should conduct an inspection to check for signs of sabotage. Sabotage may place personnel at risk, may disrupt operations or may result in other secondary risk effects. The details are covered under the facility security plan (Annex 9). In the event of an incident, the following points should be addressed:

1. Lock down the mobile BSL-2 laboratory and alert the OSRO, district health officer to notify the nearest law enforcement agency
2. Determine what has been sabotaged:
  - a. Equipment
  - b. Materials
  - c. Systems
  - d. Technology and Communications
3. Are the saboteurs violent, are they armed... how will they respond if apprehended? What risks are associated with the individuals themselves?
4. Determine what risks are connected to the act:
  - a. Explosive
  - b. Failure
  - c. Disruptive
  - d. Toxic
  - e. Structural
  - f. Information
5. What risks are presented to personnel directly, or because of secondary hazards.
6. Document and photograph sabotaged materials, assets or structures. The field deployment will be in coordination with LEAs who already have trained staff in investigative procedures along with OSRO.

## Loss of valuable and/or high-value assets

The loss of sensitive or high-value assets, equipment or information can have significant operational implications. A material and equipment inventory of equipment should be developed and conducted before use, and after decontamination after work has concluded. The Enterprise lab solution/mobile application will have an inventory management module to keep track of all consumables on daily basis. The primary responsibility lies with the designated lab in charge who also acts as safety and security focal person (SSFP). He will assign this job on rotational basis. Staff should identify which materials, resources, or equipment might be considered sensitive or of high value and attribute measures by which to protect such items. Risks may include espionage, loss, theft, damage or destruction. In the event of an incident occurring the following points should be addressed:

- Establish the nature and details of the material or item: determine how it was lost
- Determine the impact of the loss or damage to sensitive or high-value materials; both direct and peripheral
- Confirm the last location and owner responsible for the material or item
- Gain written reports from the person to whom the item was assigned
- Confirm whether the item was destroyed or was left intact at the scene or work site
- Liaise with appropriate authorities to recover the item or confirm destruction
- Take appropriate actions to mitigate the risks associated with the loss of the item, especially for communications or intelligence sensitive materials
- Confirm standard operating procedures were followed—provide a post-incident report

### **Explosion or Risk of Explosion**

In the event of explosion, all persons initiate Duck and Cover.<sup>6</sup> Follow directions from lab in charge/safety and security focal person to take appropriate action afterwards, alert the OSRO, district health officer to notify the nearest law enforcement agency. District Health Officer is the representative of local district health department. He will be the in-charge of the administrative, security and logistic arrangements during field deployment. So, they need to be alerted at first to coordinate response from local LEAs.

A VBIED is a tactic in which a vehicle is used as a delivery mechanism and can be in the form of a static vehicle, set on a timer, tilt mechanism, or remotely detonated. Or be in the form of a mobile/static suicide bomber. Standard operating procedures should be in place to limit the opportunities for unauthorized vehicles containing explosives to enter a secured area. This will include both physical measures (barriers, gates, guards) and policies and procedures set up and maintained by facility security manager. In the event of an incident occurring the following points should be addressed:

1. Take shelter (lay down, move behind, move away)—refer to explosive hazard distances diagram for details.
2. Notify emergency services immediately.
3. Establish a casualty management point if an explosion has occurred.
4. Assist casualties and walking wounded—provide casualty reports as per the communications plan.
5. Establish an incident control point to coordinate responses and meet external response groups – notify responding agencies of the location and of safe routes in.
6. Confirm there are no “secondary” devices—conduct a security sweep.
7. Implement the six Cs:

---

<sup>6</sup> Duck and Cover: This action is taken to protect staff from flying or falling debris. In the event of severe weather, staff should stay inside the laboratory. If that is not possible, they should duck under tables or lab benches and cover their heads with their arms and hands.

- a. **Confirm** the presence of the suspect device. This should be a one-person task (if appropriate) and needs to be done from a distance whenever possible. Maximum use should be made of hardcover and spotting equipment through such means as binoculars or scopes.
  - b. **Clear** the area around the device of all personnel, working from the device outwards, to 300m. Maximum use should be made of hard cover, such as buildings. No one should be in clear sight of the threat area.
  - c. **Cordon** the 300m danger area and set up an incident control point (ICP) for follow on agencies to meet at. Personnel who are being cleared from the area should be checked at random to deter additional threats.
  - d. **Control** the area inside the cordon to ensure only authorized access is achieved. Only emergency services should be allowed to breach the cordon through the control point. Any breaches of the cordon should be reported immediately to the IRT Commander.
  - e. **Check** all personnel stationed on the cordon should check their immediate area for secondary devices and hazards. Any suspicious items should be reported to the situation commander and their position marked.
  - f. **Coordinate** activities between mobile lab and emergency responders. Effective coordination is critical for the safe resolution of the situation.
8. Carry out a roll call of all employees and personnel—locate missing persons.
  9. Begin a running log of events as they occur, recording activities.
  10. Do not divulge the names of casualties until their next of kin has been notified.
  11. Provide a Serious Incident Report as soon as possible.
  12. Cordon off the site of a detonation—this is relevant for any forensic investigations, as well as mitigating the threat from any secondary devices or unexploded ordnance.

### **Fire in the Laboratory**

If there is a fire in the mobile laboratory, initiate fire extinguishing protocols within the laboratory. In case of high-fire danger, evacuate the vehicle immediately, inform the alert at 1122 or fire brigade service, so that preventative measures may be taken to prevent the fire from spreading. Notify the OSRO, district health officer to notify the nearest law enforcement agency. Use the Incident Report Template to file a post-incident report to X office/authority.

### **Fire in Surrounding Area**

If a fire is discovered in an area adjoining property, move the mobile laboratory immediately out of the vicinity to another designated safe place and notify the OSRO. Security personnel deployed will be working in liaison with external groups for early warning on fire.

### **Flooding**

If the mobile laboratory is flooded, evacuate the vehicle, and cancel all activities until water levels have receded and it is deemed safe to re-enter the lab.

### **Lockdown**

Anytime a situation develops where it is safer to keep occupants in the vehicle than to evacuate, a lockdown protocol should be followed. Examples of lockdown events include active shooter scenarios, violent protests, when directed by law enforcement and it is necessary to prevent the perpetrator(s) from entering the mobile laboratory, and more. If a lockdown is initiated, lab staff should follow suit unless given other instructions by the Law Enforcement Agency.

#### **Lockdown Procedure:**

1. [Add in SOP that describes the rapid inactivation protocol to safely cease all active bio work.]
2. Close and lock all doors and windows immediately.

3. DO NOT open doors or windows unless ordered to do so by law enforcement. Always ask for documentation from an official to confirm their identity.
4. Turn off all lights, cover windows and doors.
5. Have staff gather in areas that are out of sight from the windows as much as possible (behind doors, under the tables, in the center of the vehicle, etc.).
6. Ensure all cell phones and electronic devices are set to silent.
7. Remain in place until ALL CLEAR is given.

## Biological Events

### Reporting of Incidents Involving Biological Agents

The spill scenarios must be reported to the notified OSRO. Incidents or safety concerns can also be reported online on the Enterprise Lab Solution home page, then click on the “Report an Incident, Near-miss, or Safety Concern” link.

The following are to be reported immediately:

- i. All spills or personnel exposure incidents involving BSL-2 agents or select agents and toxins (reporting of minor spills contained in a biological safety cabinet can wait until business hours if no personnel exposure is suspected). Risk assessment tool can be accessed at Annex 10.
- ii. All personnel exposure incidents involving BSL-2 agents.
- iii. Overt exposures of personnel to BSL-2 recombinant or synthetic nucleic acid.
- iv. High-risk spills of any BSL-2 agent or biological toxin, even when released within a biological safety cabinet or other containment (elevated risk due to large volume or high potential for aerosolization).
- v. Any spill or release of a biological agent outside of a laboratory room or release to the outside environment by any route (e.g., ventilation system, sewer, or spill during transport).
- vi. Physical accidents.

The Incident Management Committee is the appropriate forum for reporting incidents in the prescribed Serious Incident Reporting template (Annex- 4) for final review and further action.

### Biohazardous Waste

Incidents involving spills or releases of biohazardous waste that result in personnel exposure, a health and safety hazard to the public or agricultural or domestic animals, or discharge to the environment, must be reported to the provincial lab focal person, the District Health Office, and IMC/NIH to take appropriate steps for its containment while referring to the standard biosafety protocols.

### Release of Biological Agents

Release of infectious agents outside of the laboratory, to the environment must be reported to OSRO, District Health Office, along with the office of the Director General Health Services and NIH to take appropriate steps for its containment while referring to the standard biosafety protocols.

### Exposure to Personnel

Personnel exposure incidents involving a causative agent of a communicable disease must be reported to OSRO, District Health Office, along with office of the Director General Health Services and NIH to take appropriate steps for its management while referring to the standard biosafety protocols as soon as possible. Reportable incidents are those that involve specific contact of an infectious agent with eyes, mouth, or other mucous membranes; parenteral contact; contact with non-intact skin; exposure to aerosols; and diagnosed illnesses known or suspected of being laboratory acquired.

### Fatalities or Hospitalizations

Any occupational incident that results in the fatality of an employee within eight hours, work-related in-patient hospitalization of one or more employees, amputation, or loss of an eye, must be reported to OSRO, District Health Office, along with office of the Director General Health Services and NIH to take appropriate steps.

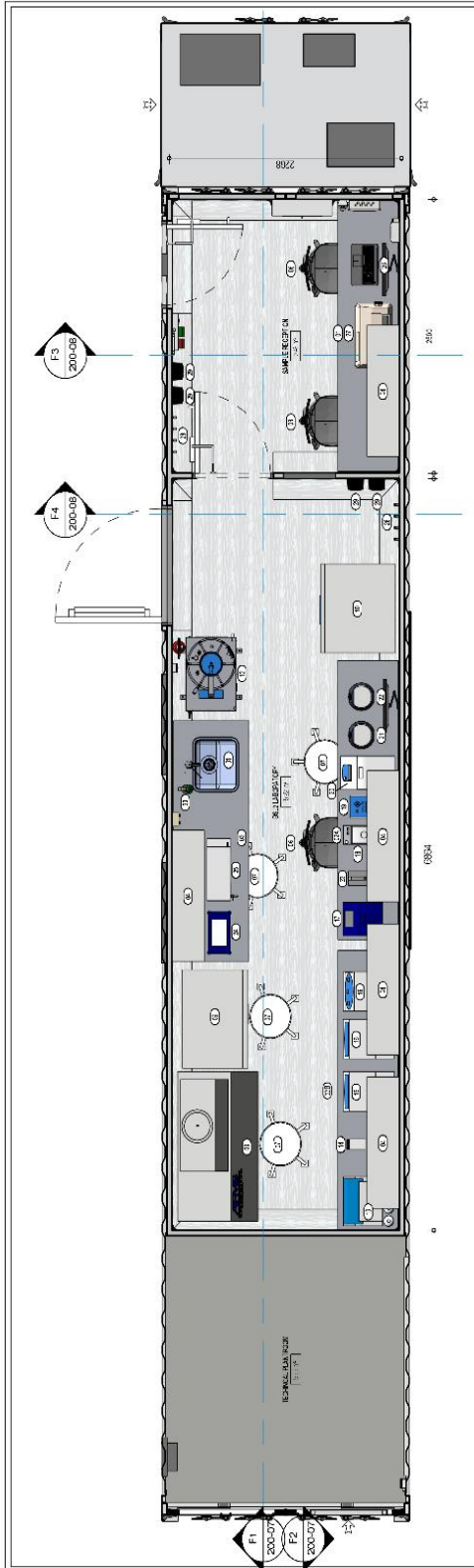
## Laboratory Emergency Preparedness Checklist

The following are recommended steps to take before an event that may result in an interruption of laboratory operations:

Sr. No.	Lab Checklist	Remarks
1.	Close fume hoods/biosafety cabinets.	
2.	Close all windows and lock all doors.	
3.	Secure/shut down all operations that could be affected by loss of electricity, water, or other services	
4.	Remove all chemicals and glassware from benchtops and store in cabinets	
5.	Remove infectious materials from biosafety cabinets, and autoclave, disinfect, or safely store them as appropriate.	
6.	Ensure that all chemicals, radioactive, and hazardous waste containers are properly covered, sealed, and in secondary containment.	
7.	Ensure all gas valves are closed. If available, shut off gas to area.	
8.	Turn off appliances, computers, hot plates, ovens, and other equipment. Unplug equipment if possible.	
9.	Check that all gas cylinders are secured. Remove regulators and use caps (if any in use).	
10.	Cover and secure or seal vulnerable equipment with plastic.	
11.	Inspect all equipment requiring uninterrupted power for electricity supplied through an uninterrupted power supply and by emergency power (emergency generator).	
12.	Secure lab notebooks and other data. Shut off and unplug sensitive electric equipment	
13.	Ensure emergency contact and phone numbers are up to date. Take laptops to a safe place.	
14.	Ensure you know how to contact your laboratory supervisor/safety coordinator/biosafety officer/lab manager	



# Annex 6: Layout plan of the mobile BSL-2 laboratory



### Lab Furniture and Equipment Schedule

Mark	Description	Length	Width	Height	Count
F1	RECEPTION DESK	2000	700	800	1
F2	LABORATORY BENCH	2500	600	800	1
F3	BIOHAZARD CABINETS	2300	1500	2100	1
F4	SAMPLE RECEPTION	2000	700	800	1
F5	LABORATORY BENCH	2500	600	800	1
F6	LABORATORY BENCH	2500	600	800	1
F7	LABORATORY BENCH	2500	600	800	1
F8	LABORATORY BENCH	2500	600	800	1
F9	LABORATORY BENCH	2500	600	800	1
F10	LABORATORY BENCH	2500	600	800	1
F11	LABORATORY BENCH	2500	600	800	1
F12	LABORATORY BENCH	2500	600	800	1
F13	LABORATORY BENCH	2500	600	800	1
F14	LABORATORY BENCH	2500	600	800	1
F15	LABORATORY BENCH	2500	600	800	1
F16	LABORATORY BENCH	2500	600	800	1
F17	LABORATORY BENCH	2500	600	800	1
F18	LABORATORY BENCH	2500	600	800	1
F19	LABORATORY BENCH	2500	600	800	1
F20	LABORATORY BENCH	2500	600	800	1
F21	LABORATORY BENCH	2500	600	800	1
F22	LABORATORY BENCH	2500	600	800	1
F23	LABORATORY BENCH	2500	600	800	1
F24	LABORATORY BENCH	2500	600	800	1
F25	LABORATORY BENCH	2500	600	800	1
F26	LABORATORY BENCH	2500	600	800	1
F27	LABORATORY BENCH	2500	600	800	1
F28	LABORATORY BENCH	2500	600	800	1
F29	LABORATORY BENCH	2500	600	800	1
F30	LABORATORY BENCH	2500	600	800	1

### Lab Furniture and Equipment Schedule

Mark	Description	Length	Width	Height	Count
F1	RECEPTION DESK	2000	700	800	1
F2	LABORATORY BENCH	2500	600	800	1
F3	BIOHAZARD CABINETS	2300	1500	2100	1
F4	SAMPLE RECEPTION	2000	700	800	1
F5	LABORATORY BENCH	2500	600	800	1
F6	LABORATORY BENCH	2500	600	800	1
F7	LABORATORY BENCH	2500	600	800	1
F8	LABORATORY BENCH	2500	600	800	1
F9	LABORATORY BENCH	2500	600	800	1
F10	LABORATORY BENCH	2500	600	800	1
F11	LABORATORY BENCH	2500	600	800	1
F12	LABORATORY BENCH	2500	600	800	1
F13	LABORATORY BENCH	2500	600	800	1
F14	LABORATORY BENCH	2500	600	800	1
F15	LABORATORY BENCH	2500	600	800	1
F16	LABORATORY BENCH	2500	600	800	1
F17	LABORATORY BENCH	2500	600	800	1
F18	LABORATORY BENCH	2500	600	800	1
F19	LABORATORY BENCH	2500	600	800	1
F20	LABORATORY BENCH	2500	600	800	1
F21	LABORATORY BENCH	2500	600	800	1
F22	LABORATORY BENCH	2500	600	800	1
F23	LABORATORY BENCH	2500	600	800	1
F24	LABORATORY BENCH	2500	600	800	1
F25	LABORATORY BENCH	2500	600	800	1
F26	LABORATORY BENCH	2500	600	800	1
F27	LABORATORY BENCH	2500	600	800	1
F28	LABORATORY BENCH	2500	600	800	1
F29	LABORATORY BENCH	2500	600	800	1
F30	LABORATORY BENCH	2500	600	800	1

**REVISIONS**

No.	Date	By	Description
1	06/09/2021	PPARELO NELWONDO	ISSUED FOR APPROVAL
2	06/09/2021	PPARELO NELWONDO	ISSUED FOR APPROVAL
3	06/09/2021	PPARELO NELWONDO	ISSUED FOR APPROVAL

**Air Filter Maintenance Services International**  
2020-2021  
 1000 North Main Street, Suite 1000  
 Columbus, GA 31906  
 Tel: +1 706 546 2222  
 Fax: +1 706 546 2222  
 Email: info@afmsi.com

**PROJECT NAME:** MODULAR BSL2 PAISTAN

**DISCIPLINE:** ARCH

**DATE:** 16/03/2022

**APPROVED BY:** [Signature]

**APPROVED BY:** [Signature]

**APPROVED BY:** [Signature]

**PROJECT NO.:** 378

**DISCIPLINE:** ARCH

**DRAWING NO.:** 201/06

**REVISION:** 3

**PAPER SIZE:** A3

**DATE DRAWN:** 06/09/2021

**DRAWN BY:** PPARELO NELWONDO

**DATE CHECKED:** 06/09/2021



# Annex 7: SOPs for Avoiding Occupational Hazards

## Occupational Health Support Service Elements

1. Preplacement Medical Evaluations
2. Vaccines
3. Periodic Medical Evaluations/Surveillance
4. Post-exposure Medical Support for Occupational Illnesses and Injuries

### Preplacement Medical Evaluations

- Workers exposed to human pathogens should receive preplacement medical evaluation
- Laboratory workers should be cognizant of potential hazards that they can encounter
- Laboratory workers should receive the previous medical history of the lab worker
- When occupational exposure to agents is a risk, collecting and storing serum samples before work should be considered
- At-risk laboratory staff will not to be involved in laboratory functions that require handling the live viruses, such as RNA extraction
- Any existing health conditions recorded, like diabetes, hypertension, and other comorbidities
- Laboratory workers should be tested if they develop any symptoms of the disease

### Vaccines

- Immunizations recommended for all laboratory workers based on risk assessment:
  - a. Seasonal influenza
  - b. COVID-19
  - c. Measles/rubella
  - d. Hepatitis B
  - e. Diphtheria
  - f. Pertussis
  - g. Varicella
- If high incidence of infection in the population and risk of transmission, then:
  - a. BCG
  - b. Meningococcus

Note:

Even if health workers have received immunizations, standard precautions still need to be followed.

### Periodic Medical Evaluations/Surveillance

- Laboratory workers should undergo medical check-ups and, if needed, tests to:
  - a. Their fitness for the work to be done
  - b. Temperature checks before entry in the labs
  - c. Any existing medical condition that may endanger their health
  - d. Detection of any occupational disease as early as possible especially COVID-19 while working with PCR testing or screening tests
  - e. Exceptional care should be taken while handling the live virus (BSL-3)
  - f. Report to your lab supervisor any issues that can put you and your colleagues in danger, stay at home if sick
  - g. Decontamination of surfaces and space after any bench work

- h. Following the manufacturer’s recommendations for use, such as dilution, contact time, and safe handling
- i. Monitor symptoms of other staff members with their testing after exposure
- j. Get immunizations as per occupational policies of the institute and planned medical check-ups

**Post-Exposure Medical Support for Occupational Illnesses and Injuries**

- Laboratory workers encouraged to seek medical evaluation for symptoms if they suspect related to their work
- Unexplained illness should be reported as presentation of occupational infections may differ from naturally acquired infections
- First aid should be provided and repeated if required
- Post exposure protocols should be developed to prevent illness in some instances
- Post-exposure Care Plan (PEP), including treatment options, testing procedures, and interpretation of laboratory results
- If PEP is not available, appropriate post-incident care tailored to the exposure and workers’ health status
- Post-exposure serologic testing may be useful

Signed:

\_\_\_\_\_  
Laboratory Manger

<b>EXPOSURE AND INJURY RESPONSE</b>	
<b>CALL 1122 FOR ANY LIFE-THREATENING EMERGENCY</b>	
<b>1. PERFORM FIRST AID</b>	
<b>Puncture, Other Wound, Skin Exposure, Needle Stick</b>	1. Wash exposed area thoroughly for 15 minutes with water and soap
<b>Eye or other mucus membrane exposure</b>	2. Use eye wash to flush eyes for 15 minutes while holding eyes open
	3. Secure work area before leaving
<b>4. GET MEDICAL HELP</b>	
<b>For specific BSL-2 + exposures</b>	1. HIV/HBV/HCV medical evaluation/treatment
<b>For injuries or non-biological exposures</b>	2. Seek medical treatment as required
<b>3. REPORT THE INCIDENT</b>	
<b>Notify the following personnel of the exposure, injury, or concern</b>	1. Provincial lab focal person and incident management committee 2. Email 3. Complete the incident reporting form

## Annex 8: Rapid Inactivation Protocols

There are three types of liquid chemical germicides for processing medical equipment and surfaces:

1. Sterilant/high-level disinfectant
2. Intermediate-level disinfectant
3. Low-level disinfectant

LAIs can be spread to laboratory employees directly or indirectly through contaminated environmental sources (e.g., air, fomites, and laboratory instruments, aerosols, and splashes). As there are multiple prerequisites for environmental transmission to occur, which is usually referred to as the chain of infection, LAIs are relatively unusual events. The presence of a pathogen with sufficient virulence, a sufficient dose of a pathogen to cause infection (i.e., infectious dose), a mechanism of pathogen transmission from the environment to the host, the correct portal of entry into a susceptible host, and the host's immune status are all requirements for environmental transmission.

Intermediate and low-level disinfectants can be used safely in most cases. Sodium hypochlorite solutions at concentrations of 500 to 6,000 parts per million (ppm), oxidative disinfectants such as hydrogen peroxide and peracetic acid, phenols, and iodophors have all been used for decontamination. Safety considerations, the use of proper personal protective equipment, hazard communication, and spill response training should all be included in chemical disinfectant procedures.

Concentrations and exposure times vary, depending on the disinfectant formulation and the manufacturer's instructions for use. See Table I for a list of chemical disinfectants and their activity levels.

Table I. Activity Levels of Selected Liquid Chemical Disinfectants

Chemical	Concentration	Activity Level
Hypochlorite	500–6,000mg/L Free available	Intermediate to high-level disinfection
Alcohols (ethyl, Isopropyl)	70%	Intermediate Level disinfection
Quaternary Ammonium Compounds	Variable	Low-level disinfection
Hydrogen peroxide	6–30%	Sterilization
Hydrogen peroxide	3–6%	Intermediate to high-level disinfection
Peracetic Acid	0.08%–0.23% with peroxide concentrations of 1–7.35%	Sterilization
Peracetic Acid	Variable	High-level disinfection
Formaldehyde	6–8%	Sterilization
Formaldehyde	1–8%	Low- to high-level disinfection
Chlorine dioxide	Variable	Sterilization
Chlorine dioxide	Variable	High-level disinfection
Phenolics	0.5%–3%	Low to intermediate level disinfection
Glutaraldehyde	Variable	Sterilization
Glutaraldehyde	Variable	Intermediate to high-level disinfection
Iodophors	30–50mg/L Free	Low to intermediate disinfection

Note:

- The above table contains the generic formulations of chemical disinfectants
- Many commercial products are available for local use
- Formaldehyde is classified as known human carcinogen and is considered to have low permissible exposure limit. Its use is limited to certain specific and controlled conditions
- Liquid and solid generic chlorine disinfectants are available (e.g., sodium or calcium hypochlorite). Rapid-acting and broad-spectrum concentrations are listed (i.e., tuberculocidal, bactericidal, fungicidal, and virucidal)
- Sodium hypochlorite, in the form of common home bleach, is a good and economical supply
- Higher concentrations are extremely corrosive as well as irritating to personnel, and should be used only in situations when spores, an excessive amount of organic material, or unusually high concentrations of microorganisms are present (e.g., spills of cultured material in the laboratory)
- The effectiveness of alcohol as an intermediate-level germicide is restricted due to its quick evaporation, which results in short-contact durations and its inability to permeate leftover organic material. These solutions are tuberculocidal, bactericidal, and fungicidal, although their virucidal spectrum varies. Items to be disinfected with alcohol should be thoroughly cleaned before being immersed for the required amount of time

---

Laboratory Manager

## Annex 9: Facility Security Plan

Version 1.0

# Mobile Bio Laboratory



## FACILITY SECURITY PLAN and Guard Force Instructions

**Country**

**Location**

**MBL Tag No**

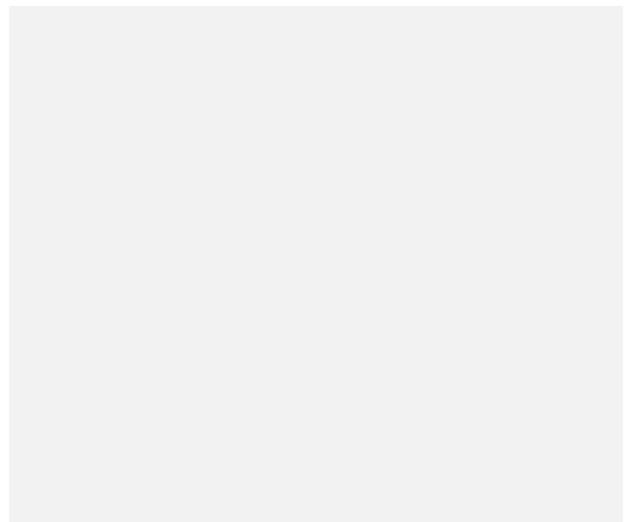
**Team Leader**

**Safety and Security Focal Person**

**Security Manager**

**Dated**

**Review Date**



# Table of Contents

## INTRODUCTION

Facility Risk Profile

### SECTION I

- 1.1 Facility Security Plan
- 1.2 Facility Specifics
- 1.3 External Supporting Groups
- 1.4 Perimeter Security
- 1.5 Stand-Too Positions
- 1.6 Access Control
- 1.7 Vehicle Access Control:
- 1.8 Pedestrian Access Control:
- 1.9 Parking
- 1.10 Security Technologies
- 1.11 MBL Security Management
- 1.12 MBL Container Protection
- 1.13 Lock and Key Security
- 1.14 Security Control
- 1.15 Power Sources
- 1.16 Sensitive Materials
- 1.17 Safe Havens and Muster Points

### SECTION II

- 2.0 Guard Force Services
- 2.1 Guard Force Mission
- 2.2 Guard Force Functions
- 2.3 Guard Organization
- 2.4 Guard Force Matrix
- 2.5 Guard Force Commander Instructions
- 2.6 Gate Guard Instructions
- 2.7 Night Guard Instructions
- 2.8 Use of Force
- 2.9 Rules of Engagement
- 2.10 Emergency Response Instructions – Attack or Intruders
- 2.11 Emergency Response Instructions – Suspect Device



## INTRODUCTION

The Facility Security Plan and Guard Force Instructions document is designed to enable the security management team to quickly define what resources and measures are required to protect staff, assets (mobile bio-laboratory, MBL), and materials within a specific operating region or city. The plan provides details on the principles of securing facilities, as well as specific reviews of the MBL holding facility. Also, this document provides instructions on managing the specific facility guard force requirements, as well as orders and instructions for those security personnel, as they relate to this facility and security requirements. An accompanying document, which illustrates the location of the facility, escape routes, stand-too positions, and safe havens, will also be developed after assessment to visualize the facility security plan and guard force deliverables.

A series of general orders for the guard force has been provided to ensure pragmatic directions and instructions are provided to guard commanders and guards. These have been provided to allow SSFP to insert native language instructions should English not be the primary language. Each member of the guard force is responsible for being fully familiar with and responsive to these general orders. These orders will not be modified or revised without the written authority of the security management team.

## Facility Risk Profile

The facility risk profile has been evaluated using the following risk table:

Risk Nature	Low	Medium	High	Serious
▪ Low-level Crime	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▪ Organized Crime	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▪ Demonstrations and Rallies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▪ Militancy or Terrorism	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▪ Explosive Attacks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▪ Armed Attacks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▪ Kidnapping and Ransom	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▪ Public Protests	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▪ Flooding	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▪ Earthquakes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▪ Fires—Natural or Manmade	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▪ Others	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Observations:

\* Note: The facility risk profile should be reviewed and updated on a scheduled basis.

# SECTION I

## I.1 FACILITY SECURITY PLAN

The term “facilities” here identifies the locations where MBL will be parked for long-term and short-term durations to perform its functions. These locations/work sites must be appropriately protected to enable staff and visitors to operate with confidence that appropriate measures are in place to safeguard them from possible threats. Facility protection is a 24/7 requirement and does not end at the completion of a workday.

This Facility Security Plan and associated Guard Instructions provides a comprehensive document that captures the physical and procedural security measures in place for this location. It captures the risk profile, nature of the site, and security technologies, structures, and manpower employed to protect people, activities, structures, and materials.

Facility Profile			
▪ The Facility Is a High-Profile Site	<input type="checkbox"/>	▪ The Facility Is a Medium-Profile Site	<input type="checkbox"/>
▪ The Facility Is a Low-Profile Site	<input type="checkbox"/>	▪ High-Profile Sites Next to Facility	<input type="checkbox"/>
▪ Facility on Major Road	<input type="checkbox"/>	▪ Facility on Back Road	<input type="checkbox"/>
<b>Observations:</b>			

Facility Type			
▪ Government Office	<input type="checkbox"/>	▪ Privately Held Location	<input type="checkbox"/>
▪ Government Hospital	<input type="checkbox"/>	▪ Warehouse and Storage	<input type="checkbox"/>
▪ Semi-Government	<input type="checkbox"/>	▪ Training Facility	<input type="checkbox"/>
<b>Observations:</b>			

Facility Vehicle Access Control			
▪ Road Ramming Run-Ups Limited	<input type="checkbox"/>	▪ Road Ramming Run-Ups High Risk	<input type="checkbox"/>
▪ Metaled Vehicle Gates	<input type="checkbox"/>	▪ Wire or Wrought Iron Vehicle Gates	<input type="checkbox"/>

▪ No Vehicle Gates	<input type="checkbox"/>	▪ Gates Have Anti Climb Devices	<input type="checkbox"/>
▪ Outer Chicanes or Bollards Used	<input type="checkbox"/>	▪ The Facility Has a Search Area	<input type="checkbox"/>
▪ Inner Anti-Ram Bollards Used	<input type="checkbox"/>	▪ The Facility Has an Airlock System	<input type="checkbox"/>
<b>Observations:</b>			

Facility Management Structures			
▪ The Facility Has an Operations Room	<input type="checkbox"/>	▪ The Facility Has a Guard Hut	<input type="checkbox"/>
<b>Observations:</b>			

Pedestrian Access Control			
▪ Has Pedestrian Access Control Gates	<input type="checkbox"/>	▪ Has a Male Pedestrian Search Area	<input type="checkbox"/>
▪ Has Inner Access Control Points	<input type="checkbox"/>	▪ Has a Female Pedestrian Search Area	<input type="checkbox"/>
<b>Observations:</b>			

Perimeter Security Measures			
▪ All Perimeter Walls Robust	<input type="checkbox"/>	▪ Most Perimeter Walls Robust	<input type="checkbox"/>
▪ Most Perimeter Walls Not Robust	<input type="checkbox"/>	▪ No Perimeter Walls Are Robust	<input type="checkbox"/>
▪ Perimeter Installed Anti-Climb Measures	<input type="checkbox"/>		
<b>Observations:</b>			

Facility Gates Security			
▪ Facility Gates Are Robust	<input type="checkbox"/>	▪ Facility Gates Are Adequate	<input type="checkbox"/>
▪ Some Facility Gates Are Not Adequate	<input type="checkbox"/>	▪ No Facility Gates Are Adequate	<input type="checkbox"/>
<b>Observations:</b>			

Facility Parking			
▪ Parking Within Inner Secured Area	<input type="checkbox"/>	▪ Secured External Parking Area	<input type="checkbox"/>
<b>Observations:</b>			

Facility Safe Havens and Escape Routes			
▪ The Facility Has an Internal Safe Havens	<input type="checkbox"/>	▪ The Facility Has External Safe Havens	<input type="checkbox"/>
▪ There Are Good External Muster Points	<input type="checkbox"/>	▪ The Facility Has Good Escape Routes	<input type="checkbox"/>
<b>Observations:</b>			

## I.2 Facility Specifics

The following specific information relates to the facility:

▪ Number of Vehicle Access Points	<input type="text"/>	▪ Number of Pedestrian Access Points	<input type="text"/>
▪ Number of Facility Access Points	<input type="text"/>	▪ Number of Parking Spaces	<input type="text"/>
▪ Number of Staff	<input type="text"/>	▪ Number of Visitors per Day	<input type="text"/>
▪ Number of Meetings Held	<input type="text"/>	▪ High Tempo Number of Visitors	<input type="text"/>
<b>Observations:</b>			

### I.3 External Supporting Groups

The availability of external supporting groups will influence the level of security and safety provided to a facility and its occupants—whether such groups are co-located or adjacent to the site, patrol the area or can provide a response or support capability. Such security and safety groups, whether military, police, medical, or commercial, can reduce the risks for that operating area on a macro and micro scale as a deterrence, as well as augment owned security and safety resources.

<b>Police</b>			
▪ Provide Robust Law Enforcement	<input type="checkbox"/>	▪ Are Considered Highly Professional	<input type="checkbox"/>
▪ Patrol the Area	<input type="checkbox"/>	▪ Are Considered Adequate	<input type="checkbox"/>
▪ Provide Good Response Capabilities	<input type="checkbox"/>	▪ Are Considered Inadequate	<input type="checkbox"/>
▪ Provide Well Placed Checkpoints	<input type="checkbox"/>	▪ Are in Close Proximity	<input type="checkbox"/>
<b>Observations:</b>			

<b>Military</b>			
▪ Provide Robust Law Enforcement	<input type="checkbox"/>	▪ Are Considered Highly Professional	<input type="checkbox"/>
▪ Patrol the Area	<input type="checkbox"/>	▪ Are Considered Adequate	<input type="checkbox"/>
▪ Provide Good Response Capabilities	<input type="checkbox"/>	▪ Are Considered Inadequate	<input type="checkbox"/>
▪ Provide Well-placed Checkpoints	<input type="checkbox"/>	▪ Are in Close Proximity	<input type="checkbox"/>
<b>Observations:</b>			

<b>Other Commercial Security Groups</b>			
▪ Are Close to The Facility	<input type="checkbox"/>	▪ Provide Robust Security Measures	<input type="checkbox"/>
▪ Will Provide Support if Needed	<input type="checkbox"/>	▪ Are Considered Professional	<input type="checkbox"/>
▪ Are Reliable if Called Upon	<input type="checkbox"/>		
<b>Observations:</b>			

<b>Emergency Services</b>			
▪ Provide Quick Response	<input type="checkbox"/>	▪ Provide Adequate Response	<input type="checkbox"/>
▪ Are Located Close to the Facility	<input type="checkbox"/>	▪ Can Reach the Facility within 3–5 minutes	<input type="checkbox"/>
▪ Have Modern Equipment in Place	<input type="checkbox"/>	▪ Are Professional and Trained	<input type="checkbox"/>
<b>Observations:</b>			

<b>Medical Support Services</b>			
▪ Provide Quick Response	<input type="checkbox"/>	▪ Provide Adequate Response	<input type="checkbox"/>
▪ Are Located Close to the Facility	<input type="checkbox"/>	▪ Can Reach the Facility within 3–5 Minutes	<input type="checkbox"/>
▪ Have Modern Equipment in Place	<input type="checkbox"/>	▪ Are Professional and Trained	<input type="checkbox"/>
<b>Observations:</b>			

## **I.4 Perimeter Security**

The perimeter of the facility will act as the first physical barrier to prevent intruders from entering the area in which company staff operate. The perimeter should have measures in place that reflect not only the risks and associated security requirements but also the profile of the site compared to other related sites within the local area. The following descriptions outline the facility perimeter security measures in place:

▪ <b>Nature of Perimeter Boundary:</b>	
▪ <b>Height of Perimeter Boundary:</b>	
▪ <b>Strengths of Boundary Measures:</b>	
▪ <b>Weaknesses of Boundary Measures:</b>	

▪ <b>Profile of Boundary:</b>	
▪ <b>Effectiveness of Boundary Measures:</b>	

## I.5 Stand-Too Positions

Stand-too locations are specified locations where guards move to when the facility is under threat. These should be predetermined, and guards should have specific places of responsibility that provide a layered defense for the facility. The following stand-too positions have been identified:

Location	When used	Guard Post
<b>Observations:</b>		

## I.6 Access Control

Access control is a critical component of security and must be done in concert with the perimeter security structure. Access points are the most vulnerable areas as they are, by design, breaches in the perimeter barriers. To mitigate the risks, several simple applications of security procedures can be taken that provide a secure perimeter while still allowing for efficient access to and from the site. In principle, the security plan should adopt the following measures where possible and appropriate:

- Limit the number of access points to the minimum needed
- Use barriers to create a serpentine approach to the entry point
- Provide a secure bunker or other firing position that can overwatch the entry point while security personnel conduct their checks
- Use a physical barrier that must be moved once access is authorized to eliminate a vehicle or person from forcing entry after they stop for a security check
- For larger sites, subdivide into smaller areas each with its own vehicle access point. This could be used for motor pools to keep heavy equipment from using the same vehicle access point

as other smaller vehicles. Entry into other portions of the site would then be done only on foot

- Limit the number of vehicles allowed entry and provide parking outside the perimeter and require visitors to enter by foot
- Establish clear control procedures for allowing pedestrians and vehicles into the site

Access Control can be considered external and internal and can be broken into the major categories of vehicle and pedestrian control measures.

## 1.7 Vehicle Access Control:

The occupants of all vehicles are to be subject to the same site access controls as apply to pedestrians. A physical barrier is to be provided at the road entrance to enable security staff, when required, to check vehicles entering and leaving. Appropriate instructions are to be issued for inspecting vehicles and their occupants by security staff. Hinges are to be designed to prevent the gate being removed. Gates should work on the double or air-locked system so that personnel enter through a secure area protected from direct fire. For larger sites, they are searched and identified and then allowed to pass through the second barrier—if the facility and profile of the neighborhood permit. All gates should be designed to protect the guard force from attack by the outside and inside of the perimeter. Unmanned gates are to be kept locked and inspected regularly. Keys of emergency exit gates must be securely held but be readily available. Manned gates are to be supervised from a position that enables the guard to communicate directly and effectively with the security control room. Emergency gates in the perimeter barrier may be required to provide safe evacuation routes. A metal screen gate may be required to allow the MBL facility to be secured at night and locked down in the event of increased hostilities. Defendable positions should be constructed to afford security personnel protection from attack. These should be strategically placed at all static guard positions. Vehicle Access Control Procedures are:

▪ Management Vehicles Searched	<input type="checkbox"/>	▪ Management Vehicles Not Searched	<input type="checkbox"/>
▪ Staff Vehicles Searched	<input type="checkbox"/>	▪ Staff Vehicles Spot Checked	<input type="checkbox"/>
▪ Visitor Vehicle Spot Checked	<input type="checkbox"/>	▪ Visitor Vehicles Always Checked	<input type="checkbox"/>
▪ Boots (Luggage Area) Checked	<input type="checkbox"/>	▪ Engine Area Checked	<input type="checkbox"/>
▪ Undercarriage Checked	<input type="checkbox"/>	▪ Bags and Luggage Checked	<input type="checkbox"/>
▪ Passengers Searched	<input type="checkbox"/>	▪ Passengers Spot Checked	<input type="checkbox"/>
▪ Gates Locked at Night	<input type="checkbox"/>	▪ Gates Locked When Closed	<input type="checkbox"/>
▪ Observed From a Defended Position	<input type="checkbox"/>	▪ Gates Left Open During Workday	<input type="checkbox"/>
<b>Observations:</b>			



## I.8 Pedestrian Access Control:

Control procedures for pedestrians, designed to prevent unauthorized entry or introduction of weapons or other contraband, are essential. All visitors and all employees are subject to personal and baggage searches, either for every person or on a spot check basis. Visitors may require guard force escorts as needed. All individuals authorized for access to MBL must display identity documents (if issued) and allow for inspection upon demand.

▪ All Pedestrians Searched on Entry	<input type="checkbox"/>	▪ Spot Checking on Entry	<input type="checkbox"/>
▪ All Pedestrians Search on Exit	<input type="checkbox"/>	▪ Spot Checking on Exit	<input type="checkbox"/>
▪ Mobile Phones Held at Gate	<input type="checkbox"/>	▪ Mobile Phones Switched Off	<input type="checkbox"/>
▪ No Photography Allowed on Site	<input type="checkbox"/>	▪ Identification Badges Issued	<input type="checkbox"/>
▪ Visitor Escorts Required	<input type="checkbox"/>		
<b>Observations:</b>			

The following equipment must be always readily available in the guard hut:

- Torch and batteries
- Packet of spare batteries
- Spare charged radio battery
- Copy of guard orders
- Room accountability list
- Map of facility with room occupancy
- Spare pens and logbook
- Weapons and guard equipment
- Blank incident reports

## I.9 Parking

Parking should be by permit only and restricted to specific parking areas away from MBL (at a minimum of 25 meters), if available. Some facilities may not have sufficient space to secure and store all the authorized vehicles for that site, or any visitors or staff member vehicles. No vehicle will be allowed access within 25 meters of an MBL parking spot. Restricted parking will be enforced by the guard force for authorized vehicles. If the staff parking lot is outside the main perimeter, then a secondary barrier will be needed to protect vehicles from attack or criminal activity. Such external parking should be secured, or watched, where possible. The following instructions are associated with this facility:

▪ Management parks on site	<input type="checkbox"/>	▪ 25-meter parking radius from MBL	<input type="checkbox"/>
▪ All staff park on site	<input type="checkbox"/>	▪ 50-meter parking radius from MBL	<input type="checkbox"/>
▪ No staff park on site	<input type="checkbox"/>	▪ No management parks on site	<input type="checkbox"/>
▪ High-profile visitors cannot park	<input type="checkbox"/>	▪ Guards monitor external parking	<input type="checkbox"/>
<b>Observations:</b>			

## I.10 Security Technologies

Security technologies are to be used to provide an additional layer of security for the facility, whether through CCTV systems, intruder detection systems, or other methods. Such systems may be low or high profile and are to be linked to response center. The extensive use of security lighting at the perimeter and the use of guard towers and patrolling security staff will increase security provision, but also the profile of the location. As such, the tradeoff between profile and security must be struck locally.

External lighting provides an effective deterrent and should be positioned so that it exposes the intruder but conceals the occupants inside the residence. Lighting should be angled away from the office areas and security positions in such a way as to illuminate the entire perimeter (in a high-risk area): the lights should shine into the eyes of any would-be intruders. Any potentially dark patches, which would otherwise give cover to an intruder approaching any buildings, should be illuminated by waist-high subdued lighting. The areas around all external doors giving access to the residence should be well illuminated to aid in identifying callers. If possible, external lights are to be connected to an alarm system so that they are switched on automatically whenever an alarm is triggered. The following security technologies are used for this site:

▪ High-profile Technologies	<input type="checkbox"/>	▪ Low-profile or Hidden Technologies	<input type="checkbox"/>
▪ CCTV Systems Used	<input type="checkbox"/>	▪ Perimeter Intruder Detection Systems Used	<input type="checkbox"/>
▪ Systems Linked to Police	<input type="checkbox"/>	▪ Inner Intruder Detection Systems Used	<input type="checkbox"/>
▪ Security Lighting Used	<input type="checkbox"/>	▪ Motion Lighting Used	<input type="checkbox"/>
▪ Alarms Silent	<input type="checkbox"/>	▪ Systems Linked to Security	<input type="checkbox"/>
▪ Alarms Overt	<input type="checkbox"/>	▪ Towers Used for Perimeter Security	<input type="checkbox"/>
<b>Observations:</b>			

## I.11 MBL Security Management

The protection of the actual asset itself is fundamental, as this provides the last physical barrier from intruders. The following office security management procedures are in place for this facility:

## I.12 MBL Container Protection

The surrounding perimeter of MBL may need to be fortified or hardened to delay or prevent unauthorized vehicle or pedestrian access, to reduce the impacts of armed attacks, or extreme cases gunfire and mortars. Structural reinforcement may be needed to protect from blast and shrapnel penetration hazards. As the MBL cannot be sufficiently reinforced, hesko barriers or sandbagging might be placed around the lab to afford satisfactory protection. All windows might require blast film attached. The following reinforcements are in place for this facility

▪ Perimeter Fence Installed	<input type="checkbox"/>	▪ Anti-Climbing Measures	<input type="checkbox"/>
▪ Perimeter Intrusion Alarm Installed	<input type="checkbox"/>	▪ Hesko Sandbags (Blast Protection)	<input type="checkbox"/>
<b>Observations:</b>			

## I.13 Lock and Key Security

Lock and key security forms a vital element in protecting assets. The number of keys in existence for each lock should be the minimum needed for essential use. Any spare keys should be accounted for and kept secure by SSFP. If a key is lost, all locks should be changed immediately. Never obtain replacement keys.

▪ Locks are robust	<input type="checkbox"/>	▪ Locks are adequate	<input type="checkbox"/>
▪ Locks are inadequate	<input type="checkbox"/>	▪ No locks are installed	<input type="checkbox"/>
<b>Observations:</b>			

## I.14 Security Control

MBL will be monitored 24/7 365 days a year through a dedicated security control room located at the GHSC-PSM office in Islamabad. The control room functions as a monitoring unit and incident management center. Also, each lab is to be in a facility with a localized internal security control room:

- Security Operations and Briefing Room
- Security Manager's Office
- Guard Hut and Rest Room
- Crisis Management Room

**Observations:**

## I.15 Power Sources

In Pakistan, power sources are unreliable, and facilities have back-up generators or their own power sources. Often, power is at best intermittent. It is therefore vital that all compounds have a system of generator power that can supply the compound with all its power requirements. There should also be a suitable backup to the main system. Both the main system and the backup should be hardened to protect

them from direct and indirect fire. Both generator systems should be located within the perimeter wall of the compound. The main and backup systems should be at separate locations within the compound to try and minimize damage in the event of attack.

- Power Sources Protected
- Power Sources Not Protected

### 1.16 Sensitive Materials

Sensitive materials or personnel records and cash should be located within a locked cabinet, room, or area to protect against theft or espionage.

- Personnel Records in Robust Locked Cabinets
- Contractual Documents Locked in Robust Cabinets
- Security Documents Locked in Robust Cabinets
- Crisis Plans and Policies Locked in Robust Cabinets

#### Observations:

### 1.17 Safe Havens and Muster Points

The facility should have a predefined internal haven where staff can shelter during a crisis event, as well as muster points where security staff can brief staff. If staff are required to exit the facility, safe routes and external muster points and safe havens should also be pre-identified.

▪ <b>Internal Safe Haven Location:</b>	
▪ <b>Muster Point:</b>	
▪ <b>Immediate External Safe Haven 1:</b>	
▪ <b>Immediate External Safe Haven 2:</b>	
▪ <b>Facility Safe Exit Routes:</b>	
▪ <b>External Muster Point:</b>	

A mapping showing these locations should be provided as an additional annex to this plan.

## SECTION II

### 2.0 GUARD FORCE SERVICES

The complexity and profile of the facility, the nature of the operating environment and associated threats, along with the number of employees and the nature and value of materials to be protected determine the number and type of security guards needed, as well as the equipment they use. Guards perform a range of security and administrative functions and represent the MBL Operations as a professional security-managed facility.

#### 2.1 Guard Force Mission

The guard force protects MBL personnel, assets, and equipment from personal harm, unauthorized entry, damage, or loss due to violent attack or theft 24 hours a day, seven days a week, for the entire duration of the contracted period of performance.

#### 2.2 Guard Force Functions

The guard forces deployed at the MBL will be required to perform several tasks, including:

- **Search:** To ensure that personnel, goods, and vehicles that are entering a site present no risks to MBL or its occupants. The types of searching could range from the use of x-ray machines to metal detectors, down to manual searching of personnel and vehicles, depending on threat levels and equipment available.
- **Control:** To ensure that only authorized persons enter the facility, and that property is not stolen from it. To manage the security requirements of the facility.
- **Patrolling:** To ensure that doors, windows, and other openings are secure, suspicious persons or circumstances are reported, and hazardous conditions such as fire or suspected intrusions are reported and dealt with.
- **Inspection:** Guards are normally required to inspect the effectiveness of staff security procedures, such as the putting away of valuable and classified items and locking classified document containers and securing areas after hours.
- **Escort:** Guards are required to escort contract workers, including cleaners, working in secure areas. Guards may also escort visitors and clients into and around the MBL site.
- **Response:** To respond to security and safety issues for protecting MBL staff and materials, property, and assets. They form a functional element of the crisis response team.
- **Protection:** To protect people and property from criminal militant or terrorist threats. To secure personnel during possible violent threats, to move staff away from danger, and to intercept hostile persons or groups.

To provide an effective static guard force, it is vital that the guard force be fully integrated into the overall security plan for that location. To achieve this and to allow the guard force to do their job, there is a logical requirement for the force to be structured with a military-style chain of command to allow the timely

passage of information, training, and tasking. All security-related incidents or important activities are to be reported to the guard commander (if deployed), who in turn will pass the information up the security management chain. Guard force personnel are employed to provide entry restriction and security measures—they are not to provide investigative services and under no circumstances is an individual to attempt to investigate unusual or suspicious activity—these must be reported to the security management team.

Patrolling will be an important function in maintaining the overall integrity of the perimeter of the facility. It will also serve to provide a monitoring operation at the site and to ensure compliance with security procedures. Patrolling should in no way be interpreted as a military action; it should be used to maintain the security of the facility and should follow the overall profile stance of the MBL profile and requirements. The following patrol measures will be implemented for this facility:

- Patrols are to be conducted in a low-profile manner
- Patrols are to be conducted in a high-profile manner
- Day patrols are to be implemented randomly
- Night patrols are to be implemented randomly
- Patrol guards are to be armed with weapons

**Observations:**

### 2.3 Guard Organization

Position	Shift 1	Shift 2	Shift 3	Rest	Total
▪ Guard Commander					
▪ Access Control Guard					
▪ Male Searcher					
▪ Female Searcher					
▪ Security Escort					

### 2.4 Guard Force Matrix

The following equipment and resources will be used for protection of MBL’s personnel and assets. The guard force matrix illustrates the nature of the guard force services provided for this facility, and the responsibilities associated with facility security personnel:

▪ Guards Armed Rifles	<input type="checkbox"/>	▪ Guards Armed Shotguns	<input type="checkbox"/>
▪ Guards Armed with Pistols	<input type="checkbox"/>	▪ Guards Armed with Batons	<input type="checkbox"/>

▪ Guards Armed with Pepper Spray	<input type="checkbox"/>	▪ Guards Unarmed	<input type="checkbox"/>
▪ Guards Uniformed	<input type="checkbox"/>	▪ Guards in Civilian Cloths	<input type="checkbox"/>
▪ Guards Have Radios	<input type="checkbox"/>	▪ Guards Have Mobile Phones	<input type="checkbox"/>
▪ Guards Linked to Control Center	<input type="checkbox"/>	▪ Guards Linked to Police	<input type="checkbox"/>
▪ Guards Linked to Quick Reaction Force (QRF)	<input type="checkbox"/>	▪ Guards Not Linked to Any Group	<input type="checkbox"/>
<b>Observations:</b>			

## 2.5 Guard Force Commander Instructions

The guard commander is responsible for the following tasks:

- Ensuring the professional conduct and performance of all guards
- Checking that weapons and ammunitions are clean, oiled, and rust free
- Briefing oncoming guards of their duties, and any incidents
- Checking all radios are serviceable, checking off going watches have recharged radios
- Checking uniforms are clean and serviceable
- Managing the guard roster
- Ensuring all guards are fit for duty
- Accounting for all guard stores
- Reporting incidents or problems to the SSFP
- Securing the facility and posting guards during an emergency
- Reporting all incidents and actions taken during an incident
- Ensuring all other guard instructions are carried out
- Ensuring guards carry the Rules of Engagement Cards

## 2.6 Gate Guard Instructions

The gate guard is responsible for the following tasks:

- Preventing unauthorized access to MBL
- Preventing the removal of unauthorized materials or goods from MBL
- Monitoring and recording all movement to and from the MBL parked location
- Carrying out random or specific searches of vehicles and persons as instructed by management

- Securing the gate as instructed during an incident or attack
- Locking and monitoring the gate at the appointed time. (See further details under “Night Duty” heading)
- Limiting work areas to clearly identify restricted/exclusion areas where contractor personnel (local labor) are not authorized without specific permission or a guard escort
- Informing visitors that no photography is permitted in the facility without permission
- Managing the entry authorization list (personnel and vehicles); names/vehicles
- Requiring large vehicles to arrive empty before entering location, i.e., trash trucks
- Verifying contents of large vehicles
- Providing alternate access control point for screening/search contractor personnel and vehicle, especially oversize vehicles if possible
- Placing loading zones away from protected assets
- Coordinating government security force entry and basic interaction
- Providing daily accountability for visitors
- Informing visitors that mobile phones must be switched off unless permission has been granted otherwise for visitors
- Holding visitors’ phones at the guard room while they are visiting

## **2.7 Night Guard Instructions**

The gate guard is responsible for the following tasks:

- Lock the gate at \_\_\_\_\_ hours and until \_\_\_\_\_ hours
- During this secure period, personnel will still be allowed to enter and exit the facility, but the guard will ensure that the gate is relocked once the movement is complete
- Ensure he has a fully charged battery for his radio and torch at the start of the shift and recharge the day shift radios
- Ensure he reports serious incidents should they occur
- Check that all doors and windows are locked at the facility–patrol the grounds
- Patrol the grounds randomly to secure the area

## **2.8 Use of Force and Rules of Engagement**

Personnel are to use physical force only under the following conditions:

- It is appropriate to the situation and the nature of any threats to people or property



- It is graduated and clear warnings are first issued
- It is used only to control a violent situation, not to punish, or be used as a retaliatory measure
- It is used to detain persons until police authorities arrive

## **2.9 Rules of Engagement**

The principles for opening fire are:

- Firearms should be used only in self-defense or in the defense of others where there is an imminent threat of death or severe injury
- A clear warning must be given of the intent to use firearms unless to do so would unduly put people at risk or would be clearly inappropriate or pointless
- Warning shots or aimed shots to wound should not be fired, since doing so increases the risk to third parties
- A written record of all orders given, and actions carried out must be made
- The use of weapons must be in accordance with government regulations and laws

## **2.10 Emergency Response Instructions – Attack or Intruders**

Regardless of the nature of the threat, the following basic measures will be taken to protect people and property during an attack or intrusion.

- Lock the gates immediately, secure access control points
- Secure the building locks doors and windows
- Direct staff to the established haven or muster point in the facility
- Move to your security stations (stand-too positions)
- If required, make your weapons ready (load and cock)
- Account for all staff; be aware some may still need to gain access to the facility
- If persons injured—provide first aid, call medical services
- Report facts to the chain of command
- If rockets or mortars have been fired, sweep the area to ensure no unexploded ordnance has landed in the facility

## 2.11 Emergency Response Instructions – Suspect Device

If a suspect or identified explosive device is found, the following procedures will be followed:

- Clear the area and cordon it off so no staff can approach the device. It should be 300 meters for line of sight, or 50 meters if buildings are between people and the device
- Establish an incident control point where the police can be met, and managers can meet. Control of all activities occurs from this position
- Ensure that staff stay away from windows as blast injuries from flying glass may occur
- Alert staff to stay away from the area
- Move staff to a safe location along a protected path
- Record the details of the device, size, shape, color, location
- Do NOT touch, open, or tamper with the package
- Do NOT use your radio within 50 meters of the package—it may set it off

# Annex I0: Risk Assessment Tool

## Risk Assessment Tool (RAT)

### Foundation Of Safe Laboratory Operation

#### Agent Hazards

Capability Of Infect (Pathogenicity)	<table border="1"> <tr> <td>Low</td> <td>Moderate</td> <td>High</td> <td>Very High</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </table>	Low	Moderate	High	Very High					0				
Low	Moderate	High	Very High											
Virulence (Causing Disease/Harm)	<table border="1"> <tr> <td>Low</td> <td>Moderate</td> <td>High</td> <td>Very High</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </table>	Low	Moderate	High	Very High					0				
Low	Moderate	High	Very High											
Severity Of the Disease	<table border="1"> <tr> <td>Low</td> <td>Moderate</td> <td>High</td> <td>Very High</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </table>	Low	Moderate	High	Very High					0				
Low	Moderate	High	Very High											
Prophylaxis Available	<table border="1"> <tr> <td>Yes</td> <td>No</td> <td>N/A</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </table>	Yes	No	N/A				0						
Yes	No	N/A												
Treatment Available	<table border="1"> <tr> <td>Yes</td> <td>No</td> <td>N/A</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </table>	Yes	No	N/A				0						
Yes	No	N/A												
Stability in the environment	<table border="1"> <tr> <td>Low</td> <td>Moderate</td> <td>High</td> <td>Very High</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </table>	Low	Moderate	High	Very High					0				
Low	Moderate	High	Very High											
Host range	<table border="1"> <tr> <td>Low</td> <td>Moderate</td> <td>High</td> <td>Very High</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </table>	Low	Moderate	High	Very High					0				
Low	Moderate	High	Very High											
Indigenous	<table border="1"> <tr> <td>Yes</td> <td>No</td> <td>N/A</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </table>	Yes	No	N/A				0						
Yes	No	N/A												
Exotic to local environment	<table border="1"> <tr> <td>Yes</td> <td>No</td> <td>N/A</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </table>	Yes	No	N/A				0						
Yes	No	N/A												
Genetic characteristics of the agent (Gmo recomb, or SNA molecules, wild types)	<table border="1"> <tr> <td>Yes</td> <td>No</td> <td>N/A</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </table>	Yes	No	N/A				0						
Yes	No	N/A												
Chemical hazard	<table border="1"> <tr> <td>Yes</td> <td>No</td> <td>N/A</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </table>	Yes	No	N/A				0						
Yes	No	N/A												
Route of transmission in laboratory	<p>Please Tick</p> <table border="1"> <tr> <td>Skin</td> <td></td> </tr> <tr> <td>Eye</td> <td></td> </tr> <tr> <td>Mucous membrane</td> <td></td> </tr> <tr> <td>Parenteral</td> <td></td> </tr> <tr> <td>Ingestion</td> <td></td> </tr> <tr> <td>Inhalation</td> <td></td> </tr> </table>	Skin		Eye		Mucous membrane		Parenteral		Ingestion		Inhalation		0
Skin														
Eye														
Mucous membrane														
Parenteral														
Ingestion														
Inhalation														
ID <sub>50</sub> / LD <sub>50</sub>	<table border="1"> <tr> <td>Low</td> <td>High</td> </tr> <tr> <td></td> <td></td> </tr> </table>	Low	High			0								
Low	High													

#### Experimental Work

Animals in the lab	<table border="1"> <tr> <td>Yes</td> <td>No</td> <td>N/A</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </table>	Yes	No	N/A				0
Yes	No	N/A						
MSDS/PSDS available, if yes provide information	<table border="1"> <tr> <td>Yes</td> <td>No</td> <td>N/A</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </table>	Yes	No	N/A				0
Yes	No	N/A						
Name of agent/toxin	<input type="text"/>							

Symptoms   
 Incubation time

Hazards Of Laboratory Procedures

Agent concentration		Low	Moderate	High	Very High	<input type="checkbox"/>	0
Suspension volume		Low	Moderate	High	Very High	<input type="checkbox"/>	0
Equipment that produce aerosols		Yes	No	N/A		<input type="checkbox"/>	0
Procedures that produce aerosols		Yes	No	N/A		<input type="checkbox"/>	0
Use of sharps		Yes	No	N/A		<input type="checkbox"/>	0
Procedures with animals (Tick any one if yes)		Yes	No	N/A		<input type="checkbox"/>	0
Bites	<input type="checkbox"/>						
Scratches	<input type="checkbox"/>						
Exposure to zoonotic agents	<input type="checkbox"/>						
Handling experimentally generated infectious aerosols	<input type="checkbox"/>						
Use of personal protective equipment (Tick any one if yes)		Yes	No	N/A		<input type="checkbox"/>	0
Lab gown	<input type="checkbox"/>						
Gloves	<input type="checkbox"/>						
Mask/face shield	<input type="checkbox"/>						
N-95	<input type="checkbox"/>						
PAPR	<input type="checkbox"/>						
Bio safety cabinets (BSCs)		Yes	No	N/A		<input type="checkbox"/>	0
Centrifuges safety cups		Yes	No	N/A		<input type="checkbox"/>	0
Sealed rotors		Yes	No	N/A		<input type="checkbox"/>	0
Pre-existing conditions (If yes give details)		Yes	No	N/A		<input type="checkbox"/>	0
Use of medicines		Yes	No	N/A		<input type="checkbox"/>	0
Immunocompromised individuals		Yes	No	N/A		<input type="checkbox"/>	0
Pregnancy		Yes	No	N/A		<input type="checkbox"/>	0
Breast feeding		Yes	No	N/A		<input type="checkbox"/>	0
Risk acceptable	<input type="checkbox"/>						

Risk not acceptable



Review Of Risk Assessment And Controls

Biosafety officers	Yes	No	N/A	0
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Subject matter expert	Yes	No	N/A	0
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
IBC (If available)	Yes	No	N/A	0
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Equivalent resource local (Safety committee)	Yes	No	N/A	0
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Proficiency Of Laboratory Staff Trained In

Standard microbiological practices	Yes	No	N/A	0
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Good laboratory practices	Yes	No	N/A	0
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Responsible conduct of staff	Yes	No	N/A	0
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Worker trained in				
BSL 1	Yes	No	N/A	0
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
BSL 2	Yes	No	N/A	0
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
BSL 3	Yes	No	N/A	0
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Experience in handling infectious material	Yes	No	N/A	0
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Correct use of BSC	Yes	No	N/A	0
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
SOPs for safe practices	Yes	No	N/A	0
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Emergency response	Yes	No	N/A	0
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Verification Of Risk Management Strategies Score

(Medical surveillance program Yes/No follow required)

Training requirements

Autoclave training	Yes	No	N/A	0
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
BSC training	Yes	No	N/A	0
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Spill training (Chemical / biological)	Yes	No	N/A	0
Fire extinguisher training	Yes	No	N/A	0
MSDS online training	Yes	No	N/A	0
CRP/ AED	Yes	No	N/A	0
Ergonomics (Basic training)	Yes	No	N/A	0
First Aid	Yes	No	N/A	0
Respiratory protection	Yes	No	N/A	0
Animal use	Yes	No	N/A	0
Transport of DGS	Yes	No	N/A	0
<b>LOW RISK</b>				<b>0</b>

Protype (RAT) developed by Prof. Dr. Shamsul Arfin Qasmi  
All Rights Reserved

# Annex I I: Field Certification Protocols for Biosafety Cabinets NSF I/ANSI/49 Standard

## Field Certification Essentials for Class II BSCs

### **BSC Tests Requirements NSF/ANSI 49-2019 Annex F**

- An American National Standard, applies to Class II, or laminar flow, biosafety cabinets designed to minimize inherent hazards in work with agents assigned to biosafety levels 1, 2, 3, or 4
- It outlines basic guidelines for their design, construction, performance, and field certification

### **When Certification is Required**

- At time of installation before being put into service
- At least annually thereafter to ensure continued proper operation
- After a cabinet has been moved (may break the HEPA filter seals)
- After maintenance repairs are made to internal parts

### **Testing and Certification Professionals**

It is important that competent individuals perform testing and certification

Education and training programs for field certifiers

NSF Field Certifier Accreditation Program

- Evaluates the proficiency of those individuals who perform routine field certification of biohazard cabinets
- Written and practical exam
- Users are assured that the cabinet has been properly certified
- Individuals are issued a certificate number
- Certificate number mentioned and posted on the BSC front

### **Certification Tests**

#### **Physical Tests Related to Containment**

1. Down flow velocity
2. Face velocity
3. HEPA filter leak test
4. Airflow smoke patterns
5. Site installation assessment tests
6. Other tests

### **Worker Comfort and Safety Tests**

- Electric leakage and ground resistance and polarity tests
- Lighting intensity test
- Vibration test
- Noise-level tests

### **Down Flow Velocity Test**

- Velocity of air moving down over workspace
- Measure air velocity at multiple points across the workspace

### **Inflow Velocity Test**

Also known as “Face Velocity”

- Determines air velocity through the work access opening
- Provide air barrier for worker “personnel protection”

### **HEPA Filter Leak Test**

Integrity of supply and exhaust filters, filter housings, filter mounting frames

- Introduce aerosol upstream of HEPA filter
- Scan downstream side of filter for leaks

### **Airflow Smoke Patterns Test**

- Visually demonstrate airflow patterns within cabinet
- Smoke source passed from one end of cabinet to the other
- Downflow test
- View screen retention test
- Work opening edge retention test
- Sash/window seal test

### **Site Installation Assessment Tests**

- Alarm functions
- Blower interlock
- Exhaust system performance (proper exhaust duct negative pressure and canopy performance)

### **Other Tests**

- Cabinet leak test
- Noise, light, vibration tests
- Test alarms
- Test interlock on Class IIB2 BSC (external fan on roof shuts down when BSC fails)

### **References:**

1. NSF/ANSI 49 - 2019 Biosafety Cabinetry: Design, Construction, Performance, and Field Certification
2. CDC/NIH Biosafety in Microbiological & Biomedical laboratories BMBL 6<sup>th</sup> edition 2020
3. BS EN 12469:2000 Biotechnology. Performance Criteria for Microbiological Safety Cabinets (British Standard)



# Annex 12: SOPS for Autoclave MOBILE BSL-2 LABORATORIES

## STANDARD OPERATING PROCEDURE (SOP)

### Template to be Used

Facility: <b>MOBILE BSL-2 LABORATORIES</b>
SOP Title: <b>Autoclave: Operation SOP</b>

Revision Number	Sections Changed	Description of Change	Date	Approved By

- **Black text** can be considered generic text
- **Red text** should be considered guidance or examples and must be reviewed and replaced with facility-specific information

### I Purpose

The purpose of this document is to establish procedures for proper use of autoclaves used by the mobile BSL-2 laboratory. Adherence to this procedure allows the autoclave to function as designed to provide the appropriate level of sterilization and/or decontamination of laboratory supplies and waste

### II Scope

The scope of this document is to provide hassle-free operations of autoclave, its cycle validation to ensure the materials are properly sterilized for further procedures in the laboratory

### **III Responsibilities**

- Laboratory supervisor/manager ensures autoclaves are carefully selected, located, operated, and maintained and that users are trained on this procedure
- Laboratory personnel who use autoclaves follow the procedures outlined in this SOP and report any problems to the laboratory supervisor/manager
- Laboratory supervisor/manager ensures that all autoclaves are installed, serviced, calibrated, and validated properly

### **IV Preparation**

#### **A Materials**

- Biohazard waste bags and containers
- Temperature indicator strips
- Steam sterilization indicator tape
- Biological indicator for steam sterilization
- Appropriate growth media or self-contained biological indicator and media ampule
- Heat-resistant gloves
- PPE as determined by risk assessment
- Mild detergent/cleaning agent
- “Out of Service” sign

#### **B Equipment**

- Autoclave, SLEDD - SERIES
- AUTOCLAVE

#### **C Records and Forms**

- Autoclave Calibration Test Report
- Autoclave Validation Test Report
- Equipment Use Log

### **V Procedure**

#### **A Routine Operations**

- Set-up procedures and cycle selection
- Safety considerations and work practices

### **VI References**

#### **A Manufacturer’s Instructions**

## Annex 13: Fire Evacuation SOPs

The following steps will enhance awareness of personnel about fire evacuation:

- Knowledge of fire exits for all personnel of the mobile laboratory
- Knowledge of electrical distribution, main circuit breakers, and detailed diagram should be displayed at any visible place in the mobile laboratory
- Knowledge of main valves of air compressor and nitrogen/oxygen supply, if any

### Location of Electrical Connections

All personnel are being regularly educated for the following:

- The location of the main power of electric supply
- Knowledge of main circuit breaker/electric switches. Their location/position and how to operate (ON/OFF)

### Assembly Area of Personnel After Evacuation

- The assembly area after evacuation of mobile laboratory structure in case of fire is the open area where it is located or an adjacent road

### Roll Call Procedure After Evacuation

After evacuation, the following roll call procedure will be followed:

- Assemble in designated area
- All laboratory staff are to be assembled in an allotted area in case of fire hazard or emergency prescribed by local administration

### Conduct of Head Count

- Laboratory manager/supervisor is responsible for taking attendance
- In case the laboratory manager/supervisor is not available, the senior most person is to perform and take the roll call of available personnel

### Submission of State

- Laboratory manager/supervisor is to report to his concerned official to brief details of evacuated personnel, their availability, and their physical condition

### (d) Comparison with Morning Attendance

- Laboratory manager/supervisor is to compare the current evacuation attendance with the morning assembly roll call and highlight the missing/absent personnel of the laboratory

### Responsibility Turning off Electrical and Gas Appliances

- All personnel should be regularly educated to ensure the safety pertaining to circuit breakers, gas valves, and turning off unused appliances

### Procedure for Reporting an Outbreak of Fire

- Activate the nearest fire alarm
- Notify personnel in the immediate vicinity
- Attend to human life in danger
- Try to extinguish the fire with the appropriate extinguisher when it is safe to do so
- Turn off the electrical equipment, shut the doors, and evacuate the area by finding and follow the emergency exit signs

- Immediately inform the fire brigade with emergency numbers of the city where the mobile laboratory is stationed
- Remember to use the emergency door **only** if you are trapped in the laboratory and if exit through the anteroom is not possible
- The sound of the fire alarm acts like a red alert
- Except the evacuation team, every person inside must evacuate

**Person Discovering the Outbreak of Fire**

Follow the following guidelines:

- Any person discovering a fire should try to put it out with the help of firefighting appliances available
- Call for assistance and shout “fire fire fire”
- Notify telephone extension \_\_\_\_\_ of the location by giving location and type of fire
- If the fire is extinguished, then the person extinguishing the fire is to inform on telephone Ext / \_\_\_\_\_ that he discovered a fire and has extinguished it
- If the fire started within your work area, document in detail and submit the incident report form

**Conduct of Evacuation Drill**

Laboratory supervisor/safety coordinator is to carry out the evacuation drills by following the above-stated procedure on fire hazard/emergency annually with intimation to the following responsible officers:

- |                       |                    |
|-----------------------|--------------------|
| 1. Lab director       | Phone number _____ |
| 2. Safety coordinator | Phone number _____ |

Signed and approved by

\_\_\_\_\_  
Laboratory Director

## Annex I 4: SOPs for Laundry

### Best Practices for Laundry Handling:

The following articles, if contaminated, will require laundering:

- Lab coats
- Reusable gowns
- Uniforms (dedicated)
- Towels (if in use)

The affiliated public health care facility designated for the mobile laboratory can be used to clean contaminated clothing and other articles that require laundering. Services can be found in designated locations.

The following laundering requirements must be met:

- Handle contaminated laundry as little as possible, with minimal agitation
- Place wet contaminated laundry in leak-proof, labeled or color-coded containers before transport to laundry
- Always wear reusable rubber gloves before handling soiled laundry (e.g., lab coats, gowns, towels)
- Never carry soiled laundry items against the body. Always place it in the designated color-coded containers
- Carefully roll up soiled laundry items to prevent contamination of the air, surfaces, and cleaning staff. Do not shake linen
- Place contaminated laundry into a clearly labeled, leak-proof container (e.g., bag, bucket) in the laboratory working area. Do not transport it by gloved hand outside the laboratory where it was used
- Reprocess (i.e., clean and disinfect) the designated container after each use

Signed:

---

Laboratory Manager  
Phone No.



## Annex 15: Rapid Inactivation Protocols

There are three types of liquid chemical germicides for processing medical equipment and surfaces,

1. Sterilant/high-level disinfectant
2. Intermediate-level disinfectant
3. Low-level disinfectant

Laboratory-associated illnesses (LAIs) can be spread to laboratory employees directly or indirectly through contaminated environmental sources (e.g., air, fomites, and laboratory instruments, aerosols, and splashes). As there are multiple prerequisites for environmental transmission to occur, which is usually referred to as the chain of infection, LAIs are relatively unusual events. The presence of a pathogen with sufficient virulence, a sufficient dose of a pathogen to cause infection (i.e., infectious dose), a mechanism of pathogen transmission from the environment to the host, the correct portal of entry into a susceptible host, and the host's immune status are all requirements for environmental transmission.

Intermediate- and low-level disinfectants can be used safely in most cases. Sodium hypochlorite solutions at concentrations of 500 to 6,000 parts per million (ppm); oxidative disinfectants such as hydrogen peroxide and peracetic acid; phenols; and iodophors have all been used for decontamination. Safety considerations, the use of proper personal protective equipment, hazard communication, and spill response training should all be included in chemical disinfectant procedures.

Concentrations and exposure times vary depending on the disinfectant formulation and the manufacturer's instructions for use. See Table I for a list of chemical disinfectants and their activity levels.

Table I. Activity Levels of Selected Liquid Chemical Disinfectants

Chemical	Concentration	Activity Level
Hypochlorite	500–6,000mg/L Free available	Intermediate to high-level disinfection
Alcohols (ethyl, Isopropyl)	70%	Intermediate-level disinfection
Quaternary Ammonium Compounds	Variable	Low-level disinfection
Hydrogen peroxide	6–30%	Sterilization
Hydrogen peroxide	3–6%	Intermediate to high-level disinfection
Peracetic Acid	0.08%–0.23% with peroxide concentrations of 1–7.35%	Sterilization
Peracetic Acid	Variable	High-level disinfection
Formaldehyde	6–8%	Sterilization
Formaldehyde	1–8%	Low- to high-level disinfection
Chlorine dioxide	Variable	Sterilization
Chlorine dioxide	Variable	High-level disinfection
Phenolics	0.5%–3%	Low to intermediate level disinfection
Glutaraldehyde	Variable	Sterilization
Glutaraldehyde	Variable	Intermediate to high-level disinfection
Iodophors	30–50mg/L Free	Low- to intermediate-level disinfection

## Note:


- The above table contains the generic formulations of chemical disinfectants
- Many commercial products are available for local use
- Formaldehyde is classified as a known human carcinogen and is considered to have low permissible exposure limit; its use is limited to certain specific and controlled conditions
- Liquid and solid generic chlorine disinfectants are available (e.g., sodium or calcium hypochlorite). Rapid-acting and broad-spectrum concentrations are listed (i.e., tuberculocidal, bactericidal, fungicidal, and virucidal)
- Sodium hypochlorite, in the form of common home bleach, is a good and economical supply. Higher concentrations are extremely corrosive as well as irritating to personnel, and should be used only in situations when spores, an excessive amount of organic material, or unusually high concentrations of microorganisms are present (e.g., spills of cultured material in the laboratory)
- Alcohol's effectiveness as an intermediate-level germicide is restricted due to its quick evaporation, which results in short-contact durations, and their inability to permeate leftover organic material. They are tuberculocidal, bactericidal, and fungicidal rapidly, although their virucidal spectrum varies. Items to be disinfected with alcohols should be properly cleaned before being immersed for the required amount of time

---

Laboratory Manager



## Annex 16: Technical Working Group for Mobile BSL-2 labs

  
**F.1-5/2022/PHLD-Admn**  
**Public Health Laboratories Division**  
**NATIONAL INSTITUTE OF HEALTH, ISLAMABAD**  
**Ministry of National Health Services, Regulations & Coordination**  
**Ph: (92-051) 9255238 Fax: (92-051) 9255099**  


---

**National Focal Point for International Health Regulations**

16<sup>th</sup> May 2022

### NOTIFICATION

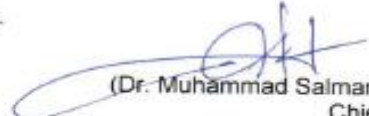
**Subject: Constitution of Technical Working Group (TWG) for Mobile BSL-2 Labs**

With immediate effect and until further orders, a Technical Working Group (TWG) has been constituted with defined TORs to oversee the modalities pertaining to mobile BSL-2 labs installation, maintenance, deployment and quality assurance etc donated by USAID to Pakistan. The TWG for Mobile BSL-2 Labs comprises of the following members:

i.	Maj. Gen. Prof. Aamer Ikram, Executive Director, NIH Islamabad	Chairman
ii.	Dr. Muhammad Salman, Chief PHLD, NIH Islamabad	Member
iii.	Dr. Faheem Tahir, PSO, PHLD, NIH	Member
iv.	Dr. Massab Umair, SSO, Virology PHLD, NIH	Member
v.	Gisele Irola, US Department of State, US Embassy, Islamabad	Member
vi.	Amanda Balish, Center for Disease Control (CDC), HQ Lab subject matter expert	Member
vii.	Troy A Krik, ODRP	Member
viii.	Dimitrius A Huntspon, ODRP	Member
ix.	Ranissa V Adityavarman, ECON	Member
x.	Dr. Muhammad Tariq, Country Director, USAID GHSC-PSM	Member
xi.	Dr. Hasnain Javaid, Focal Person for Provincial Public Health Reference Lab, Punjab	Member
xii.	Dr. Saeed Khan, Focal Person for Provincial Public Health Reference Lab, Sindh	Member
xiii.	Dr. Yasir Yousafzai, Focal Person for Provincial Public Health Reference Lab, KPK	Member
xiv.	Mr. Noor Sade Khan, Focal Person for Provincial Public Health Reference Lab, B.tan	Member

2. The Terms of References (TORs) for the subject TWG will be as follows:
- i. To oversee the modalities pertaining to mobile BSL-2 labs installation, deployment, maintenance and quality assurance etc.
  - ii. To determine the type of testing kits required by the labs
  - iii. To develop a forecast of testing kits required by the labs
  - iv. To endorse operating procedures developed for deployment of these labs
  - v. To carry out need-based assessment of supplies/ kits/ consumables
  - vi. To provide guidance on maintenance of labs

This issues with the approval of Executive Director, NIH.

  
 (Dr. Muhammad Salman)  
 Chief  
 Public Health Laboratories Division

**Distribution:**

All members of TWG



# KEY CONTRIBUTORS

## **Government Officials**

1. Prof. Aamer Ikram, Executive Director, National Institute of Health, Islamabad
2. Dr. Muhammad Amjad Khan, Coordinator CEOH (Center for Environmental and Occupational Health) National Institutes of Health, Islamabad
3. Dr. Muhammad Salman, Chief, Public Health Division, National Institute of Health, Islamabad
4. Prof. Jawad Ahmed, Dean Basic Health Sciences, Khyber Medical University, Lahore
5. Dr. Hasnain, In charge, Public Health Laboratories, Lahore
6. Prof. Saeed Khan, In charge, Public Health Laboratories, Ojha Institute, Dow Medical University, Karachi

## **USAID Global Health Supply Chain Program–Procurement and Supply Management (GHSC-PSM) Project**

1. Dr. Muhammad Tariq, Country Director
2. Prof. Dr. Shamsul Arfin Qasmi, Biosafety Laboratory Expert
3. Prof. Dr. Muhammad Tahir Khadim, Pathologist/ Laboratory Expert
4. Ms. Ambreen Khan, Director, Basic Health Services & MEL
5. Mr. Masood Anwar, Director, TO4
6. Mr. Nabeel Ahmed Maqbool, Director, Vaccine Preventable Infectious Diseases
7. Dr. Muhammad Ahmed Isa, UHC Advisor
8. Dr. Mohsin Saeed Khan, Advisor







**USAID**  
FROM THE AMERICAN PEOPLE

**USAID GLOBAL HEALTH SUPPLY CHAIN PROGRAM**  
Procurement and Supply Management



9 786277 638030