NATIONAL LABORATORY BIOSECURITY ASSESSMENT AND MONITORING CHECKLIST

(IN THE FRAMEWORK OF THE BIOLOGICAL WEAPONS CONVENTION)

Collaboration between

STRIDE®

UNODA
United Nations Office for Disarmament Affairs

National Institute for Public Health and the Environment
Ministry of Health, Welfare and Sport

NATIONAL LABORATORY BIOSECURITY ASSESSMENT AND MONITORING CHECKLIST (IN THE FRAMEWORK OF THE BIOLOGICAL WEAPONS CONVENTION)

First Edition, 2018

Published by:

Science and Technology Research Institute for Defence (STRIDE)
Ministry of Defence Malaysia
Kompleks Induk STRIDE, Taman Bukit Mewah Fasa 9
43000 Kajang Selangor

Tel: (603) 8732 4400

Website address: http://stride.gov.my/

ISBN: 978-967-16592-1-2

CONTENTS

EDITORIAL BOARD

Kathryn Tham Bee Lin
Senior Research Officer
Science and Technology Research Institute for Defence (STRIDE)
Ministry of Defence

Kumravani Santhirangathan
Medical Laboratory Technologist &
Safety and Health Officer (DOSH)
KPJ LabLink Medical Laboratory Johor

Loong Shih Keng
Research Officer
Tropical Infectious Diseases Research and Education Centre (TIDREC)
University of Malaya

Nor Yasmin binti Abd Rahaman
Senior Lecturer
Faculty of Veterinary Medicine
Universiti Putra Malaysia

Noor Faizul Hadry bin Nordin
Assistant Professor
International Institute for Halal Research and Training (INHART)
International Islamic University Malaysia

Priya Madhavan
Senior Lecturer
Faculty of Health and Medical Sciences
Taylor's University

Raha binti Ahmad Raus
Associate Professor
Faculty of Engineering
International Islamic University Malaysia

Rahizan binti Issa
Senior Research Officer
Institute for Medical Research
Ministry of Health

Saleha binti Shahar
Lecturer
Faculty of Biosciences & Medical Engineering
Universiti Teknologi Malaysia

Salmi Afidah binti Shabuddin
Science Officer
Biotechnology Research Institute
Universiti Malaysia Sabah

Tan Cheng Siang
Senior Lecturer
Faculty of Medicine and Health Sciences
Universiti Malaysia Sarawak

Venugopal Balakrishnan
Associate Professor
Institute for Research in Molecular Medicine
Universiti Sains Malaysia

W. Nur Afiza binti W. Mohd Arifin
Science Officer
National Public Health Laboratory
Ministry of Health

Wee Seng Kew
Senior Lecturer
Faculty of Bioengineering and Technology
Universiti Malaysia Kelantan

Wong Eng Hwa
Senior Lecturer
Faculty of Health and Medical Sciences
Taylor's University

Yuwana Podin
Senior Lecturer
Institute of Health and Community Medicine
Universiti Malaysia Sarawak

ADVISORS

Rik Bleijs
Head of Biosecurity Office
National Institute for Public Health and the Environment
Netherlands

Sabrina Brizee
Biosafety and Biosecurity Project Officer
National Institute for Public Health and the Environment
Netherlands

ACKNOWLEDGEMENT

This National Laboratory Biosecurity Assessment and Monitoring Checklist was developed during the Workshop on Laboratory Biosecurity Assessment, Implementation and Monitoring held on 9-11 April 2018 (1st phase) and 26-28 July 2018 (2nd phase), co-organised by The Science and Technology Research Institute for Defence (STRIDE), Ministry of Defence and the Implementation Support Unit (ISU), Biological Weapons Convention (BWC), United Nations Office for Disarmament Affairs (UNODA), and sponsored by the European Union by which Malaysia was one of the BWC state parties that were selected through the Extended Assistance Programmes offered as part of the European Union Council Decision 2016/51 in support of the Biological Weapons Convention (BWC).

STRIDE would like to acknowledge the European Union for the generous financial support, and the Implementation Support Unit especially to Mr Daniel Feakes, Chief of the Implementation Support Unit and Ms Ana Izar, Political Affairs Officer of the BWC for supporting Malaysia in our effort to strengthen our implementation of the BWC at the national level.

STRIDE also appreciates the expert guidance of Dr Rik Bleijs and Miss Sabrina Brizee from the Netherlands Biosecurity Office, National Institute for Public Health and the Environment throughout the process of developing this document.

STRIDE would also like to recognise the contributions of all national experts and those who are involved directly or indirectly in the formulation and preparation of this document.

INTRODUCTION

Article IV of the Biological Weapons Convention (BWC) mandates that every state party shall "take any necessary measures to prohibit and prevent the development, production, stockpiling, acquisition or retention of biological agents or equipment for the purpose of employing them as a biological weapon".

Malaysia as a state party to the BWC has taken many initiatives to strengthen national measures to fulfil our obligations towards the BWC. The Science and Technology Research Institute for Defence (STRIDE), Ministry of Defence, as the lead technical agency in Malaysia for the BWC, has been actively promoting and implementing national measures focusing on biosecurity, biorisk management and biothreats reduction. STRIDE has identified the need to address the concern of ensuring laboratory safety and security and establishing stronger systems to detect and prevent deliberate release of biological agents. As laboratory capacity and capabilities grow, additional attention should be paid to the potential for accidental and deliberate releases of valuable biological materials and on the broad needs around laboratory operational, regulatory, and physical security as well as personnel monitoring programmes.

It is crucial for laboratories in the country that are handling valuable biological materials to develop a comprehensive biorisk management programme and be given the necessary support and tools to assess and monitor their laboratory biosecurity implementation. With this in mind, the development of a National Laboratory Biosecurity Assessment and Monitoring Checklist was proposed by STRIDE. Expert guidance and assistance was granted to Malaysia through the European Union Extended Assistance Programmes offered as part of the European Union Council Decision 2016/51 in support of the Biological Weapons Convention (BWC).

The main objective of this checklist is to enhance Malaysia's capacity in the area of biosecurity by developing a comprehensive biosecurity checklist for laboratory assessments and monitoring. The checklist covers the eight pillars of biosecurity; management, biosecurity awareness, physical security, accountability for materials, information security, transport security, personnel reliability, and emergency response. The checklist will assist laboratories, especially high containment laboratories that are handling valuable biological materials, to assess the current level of biosecurity and identify gaps in the existing biosecurity programme; monitor the biosecurity programme efficiency and effectiveness as well as ensure compliance with national and international standards.

Through this practical approach, institutions will be able to conduct assessments and monitor their biosecurity programme to ensure they have the necessary biosecurity measure implemented to prevent potentials for accidental and deliberate releases of valuable biological materials. This checklist is also intended for assessors who are performing laboratory biosecurity assessments. This initiative will ensure a sustainable culture of scientific responsibility and most importantly show Malaysia's commitment to fulfil national obligations and enhance Malaysia's national capacity to implement the BWC.

DEFINITIONS

Accountability for Materials means the control of material which comprises both procedural and physical measures for both material and relevant information. Accountability requires a one-to-one correspondence between materials and people, together with a system of records, reporting and audit.

Awareness means knowledge and perception of the importance of biosecurity among personnel that is essential for identifying odd situations in the workplace that could form a threat to the organisation or to society at large, such as importance of protecting high-risk material, information, data and work processes.

Biohazard means the potential source of harm caused by biological agents or toxins. (Source: CWA 15793:2011)

Biological Emergencies means emergency that occurs when biological agents or toxins are released during an accident or attack.

Biosafety means the application of knowledge, techniques and equipment to prevent personal exposure to potentially infectious agents or biohazards. Biosafety defines the containment conditions under which laboratory workers can safely manipulate infectious agents. The objective of containment is to confine biohazards and to reduce the potential exposure of the laboratory worker to potentially infectious agents. Laboratory biosafety describes the containment principles, technologies and practices that are implemented to prevent the unintentional exposure to pathogens and toxins, or their accidental release.

Biorisk Assessment means a process of evaluating the biorisk(s) arising from a biohazard(s), taking into account the adequacy of any existing controls, and deciding whether or not the biorisk(s) is acceptable. (Source: CWA 15793:2011)

Biorisk Management means the analysis of ways and development of strategies to minimise the likelihood of the occurrence of biorisks. The management of biorisk places responsibility on the facility and its manager to demonstrate that appropriate and valid biorisk reduction (minimisation) procedures have been established and are implemented. A biorisk management committee should be established to assist the facility director in identifying, developing, and researching biorisk management goals. (Source: WHO Laboratory Biosecurity Guidance, 2006)

Biosecurity means measures aimed at the protection, control and accountability for valuable biological materials (VBM) and the technologies and information within laboratories, in order to prevent their unauthorised access, loss, theft, misuse, diversion or intentional release (Source: WHO Laboratory Biosecurity Guidance, 2006)

(Note: biosecurity is restricted to laboratory biosecurity; laboratory includes animal and manufacturing facilities, and does not include all aspects of biosecurity in the sense of national or regional control measures to prevent the dissemination of alien species and pathogens.)

Biosecurity Oversight Committee means an appointed congressional body that is responsible to supervise, inspect, administrate, manage and control the matters related to biosecurity concerns.

Chain of Custody means the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence.

Competent means having appropriate education, training, skills and experience. (Source: ISO 9000:2005)

Corrective Action means action to eliminate the cause of a detected non-conformity or other undesirable situation. The procedures take effect immediately following an incident that involves biological substances and include a person or group to whom the follow-up for corrective action is assigned; determining the cause of non-conformities; evaluating the action to ensure that non-conformities do not recur; determining and implementing action needed; recording and reviewing corrective actions taken. (Source: OHSAS 18001:2007 & CWA 15793:2011)

Dual Use Research ("DUR") is defined as research conducted for legitimate purposes that generate knowledge, information, technologies, and/or products that could be utilised for both benevolent and harmful purposes. (Source: National Science Advisory Board for Biosecurity (NSABB)'s 2007 Report)

Emergency Response Plan means a course of action developed to mitigate the damage of potential events that could endanger an organisation's ability to function. Such a plan should include measures that provide for the safety of personnel and, if possible, property and facilities.

Graded Protection means physical security that manifested in concentric rings of increasing security spanning from outside to inside the facility.

Information Security means policies and procedures for handling sensitive details on valuable biological materials and other sensitive information that may include laboratory security plans and inventories, and storage locations of valuable biological materials.

Management means organisation's implementation, compliance with, and maintenance of a biosecurity management system that contain procedures and rules including employees' roles and responsibilities.

Material Transfer Agreement (MTA) means a contract that governs the transfer of tangible research materials between two organisations, when the recipient intends to use it for his or her own research purposes. The MTA defines the rights of the provider and the recipient with respect to the materials and any derivatives.

Organisation means company, corporation, firm, enterprise, authority or institution, or part or combination thereof, whether incorporated or not, public or private, that has its own functions and administration. (Source: OHSAS 18001:2007)

Personnel Reliability means policies and procedures that define the roles, responsibilities and authorities of laboratory personnel who need to handle, use, store, transfer and/or transport valuable biological materials, and the manner in which the organisation ensures that individuals are appropriate for the positions they hold.

Personnel Reliability Policy means a security, medical and psychological evaluation programme designed to permit only the most trustworthy individuals to have access to the protected materials.

Physical Security means the assurance of safety from physical intrusion. It comprises of engineering, structural and security personnel elements intended to select, control and document access to laboratories and to the materials they contain, and to limit improper removal of valuable biological materials and equipment.

Preventive Action means action to eliminate the cause of a potential non-conformity or other undesirable potential situation. The procedure is taken in response to the results of incident investigations, exercises, drills, or other reviews, and includes determining the potential non-conformities and their causes; evaluating the need for action to prevent occurrence of non-conformities; determining a person or group to whom the preventive action is assigned; determining and implementing preventive action needed; recording and reviewing preventive action taken. (Source: OHSAS 18001:2007 & CWA 15793:2011)

Response means details of how to act in the event of a biological incident, accident or emergency. This relates both to internal arrangements as well as to arrangements with emergency services outside the organisation.

Response Plan means a plan of action for the efficient deployment and coordination of services, agencies and personnel to provide the earliest possible response to an emergency.

Risk Assessment means process of evaluating the risk(s) arising from a hazard(s), taking into account the adequacy of any existing controls and deciding whether or not the risk(s) is acceptable. (Source: OHSAS 18001:2007)

Secured Area is a designated area gazetted by an organisation in which access into and out of is controlled and can be monitored.

Self-Closing means closing automatically especially of a door.

Transport Security means procedures and practices to correctly categorise, package, document and safely and securely transport valuable biological materials from one place to another using any type of transport involving the use of public roads, waterways and air, following applicable national and/or international regulations.

Valuable Biological Materials means biological materials that require (according to their owners, users, custodians, caretakers or regulators) administrative oversight, control, accountability, and specific protective and monitoring measures in laboratories to protect their economic and historical (archival) value, and/or the population from their potential to cause harm. VBM may include pathogens and toxins, as well as non-pathogenic organisms, vaccine strains, foods, genetically-modified organisms (GMOs), cell components, genetic elements, and extraterrestrial samples. (Source: WHO Laboratory Biosecurity Guidance, 2006)

Whistle-Blower means any person who makes a disclosure of improper conduct to the enforcement agency. (Source: Whistle-blower Protection Act 2010)

BRIEF DESCRIPTION OF THE BIOSECURITY PILLARS

Management: Management plays a crucial role in getting ready and implementing policy on the pillars of biosecurity. If management is alert to the benefits of an efficient and effective biosecurity policy, this will facilitate the implementation and monitoring of biosecurity measures. This involves formulating policies and procedures, and assignment of roles and responsibilities to personnel with regard to biosecurity or biorisk management.

Biosecurity Awareness: Personnel have to be aware of the risks they are exposed to and the corresponding measures that can be taken when working with valuable biological materials (VBM). The awareness permits personnel to assist in determining risk, remain vigilant and adhere to the rules and procedures, as well as assess potential dual use risks, recognise abnormal phenomena and hold colleagues accountable for their behaviour.

Physical Security: The physical security focuses on authorisation, access control, and physical security measures with the objective to protect the in-house valuable biological materials (VBM). Receptionist, security personnel, and locks and closed-circuit televisions (CCTVs) are types of physical security that are crucial in preventing unauthorised people to obtain access to VBM.

Accountability for Materials: Strategies and measures are required to determine how storage, utilisation and destruction of valuable biological materials (VBM) can be secured in an organisation. Identification, registration and active management of the VBM is important to ensure the VBM is stored in a controlled and secure manner as well as making it difficult for unauthorised persons to immediately locate and identify the VBM. This accountability for materials pillar focuses on measures to prevent or restrict access to the material.

Information Security: Information security consists of three key concepts, i.e. Availability, Integrity and Confidentiality (AIC). 'Availability' shields the security of systems and manages the risks of failures, malfunctions and incidents. 'Integrity' (or reliability) guarantees that information is correct and updated. 'Confidentiality' (or exclusivity) ensures that only authorised persons have access to systems and data. Information security does not stand alone but overlaps with other pillars like physical security and biosecurity awareness.

Transport Security: Transport security consists of measures and strategies for the safety of the valuable biological materials (VBM) throughout transport. During the transportation process, neither the shipper nor the receiver has physical control of the material. For physical transport of VBM by road, water, rail and air, national/international laws and regulations are in force.

Personnel Reliability: Reliable, well-trained personnel are indispensable for biosafety and biosecurity management within an organisation. The policy of an organisation concerning personnel reliability should encompass a selection procedure for new personnel, temporary employees, external employees, and maintenance personnel. Security risks can be mitigated by implementing a thorough selection procedure and an acceptable background screening for personnel handling confidential information or valuable biological materials. In addition to physical security control measures, personnel who are conscious and aware of their surrounding also contribute to a secured environment.

Emergency Response: The emergency response service of an organisation contributes to avoiding and battling incidents, accidents and emergencies with valuable biological materials. Emergency response plans are crucial and provide guidance to an emergency response service of an organisation. A response plan describes the course of action and coordination of personnel and services involved in internal and external emergency response activities.

REFERENCES

British Standards Institution. (2007). *Occupational Health and Safety Management System - Requirements (OHSAS 18001:2007).* United Kingdom: British Standards Institution

Centre for Biosecurity and Biopreparedness. 2015. *An Efficient and Practical Approach to Biosecurity.* https://www.biosecurity.dk/fileadmin/user_upload/PDF_FILER/ Biosecurity_ book/An_efficient_and_Practical_approach_to_Biosecurity_web1.pdf

Centers for Disease Control and Prevention. 2009. *Biosafety in Microbiological and Biomedical Laboratories 5th edition: Section VI - Principles of Laboratory Biosecurity.* Atlanta: Centers for Disease Control and Prevention

European Committee for Standardization (CEN). 2011. *Laboratory Biorisk Management - CEN Workshop Agreement 15793*. Brussels: European Committee for Standardization

European Committee for Standardization (CEN). 2012. *Laboratory Biorisk Management Guidelines for the Implementation of CWA 15793:2008 - CEN Workshop Agreement 16393*. Brussels: European Committee for Standardization

Information Systems Audit and Control Association (ISACA). 2018. *Physical security checklist survey*. http://www.isaca.org/Groups/Professional-English/physical-security/ Group Documents/physicalsecurity.pdf

International Air Transport Association. 2018. *Dangerous Goods Regulations.* Quebec, Canada: IATA.

International Organization for Standardization (ISO). 2005. *Quality Management Systems – Fundamentals and Vocabulary (ISO 9000:2005)*. Geneva: International Organization for Standardization.

Malaysia. 2010. Whistleblower Protection Act. (Act 711).

Ministry of Health. 2012. *Standard Operating Procedure for Transport of Biological Specimens in Malaysia - 1st Ed.* Malaysia: Ministry of Health

National Research Council. 2010. *Understanding Biosecurity: Protecting Against the Misuse of Science in Today's World*. Washington, DC: The National Academies Press.

National Science Advisory Board for Biosecurity (NSABB). 2007. *Proposed Framework for the Oversight of Dual Use Life Sciences Research: Strategies for Minimizing the Potential Misuse of Research Information*. https://fas.org/biosecurity/resource/documents/ NSABB%20draft%20guidelines%20on%20dual%20use%20research.pdf

Office of the Under Secretary of Defense. 2009. *Report of the Defense Science Board Task Force US Department of Defense Safety and Security Program.* https://fas.org/irp/agency/dod/dsb/biosafety.pdf

Organisation for Economic Cooperation and Development (OECD). 2012. *Whistleblower Protection: Encouraging Reporting.* http://www.oecd.org/cleangovbiz/toolkit/50042935.pdf

Public Health Agency of Canada. 2016. *Canadian Biosafety Guideline - Developing a Comprehensive Biosecurity Plan.* http://canadianbiosafetystandards.collaboration.gc.ca/

Royal Netherlands Academy of Arts and Sciences. 2008. *Code of Conduct for Biosecurity* Amsterdam: Royal Netherlands Academy of Arts and Sciences

Salerno, R. M., Gaudioso, J. and Brodsky, B. H. 2007. *Laboratory Biosecurity Handbook*. Florida: CRC Press.

Sandia National Laboratories. 2014. *Laboratory Biosafety and Biosecurity Risk Assessment Technical Guidance Document.* http://www.aam.org.ar/descarga-archivos/Laboratory-Biosafety-Biosecurity-Guidance.pdf

The Netherlands Biosecurity Office. 2018. *Biosecurity Self-scan Toolkit.* http://www.biosecurityselfscan.nl/

The Netherlands Biosecurity Office. 2018. *Biosecurity Vulnerability Scan.* http://www.biosecurityvulnerabilityscan.nl/

World Health Organization. 2004. *Laboratory Biosafety Manual*. Geneva: World Health Organization

World Health Organization. 2006. *Biorisk Management: Laboratory Biosecurity Guidance*. Geneva: World Health Organization

World Health Organization. 2010. *Responsible Life Sciences Research for Global Health Security: A Guidance Document*. Geneva: World Health Organization

GENERAL INSTRUCTIONS FOR FILLING OUT THE CHECKLIST

The checklist is designed in the form of questionnaire covering the eight pillars of biosecurity to provide an indication of the current level of biosecurity of an organisation. The assessment is recommended to be conducted by a group consisting of different levels of personnel (e.g. top management, biosafety/biorisk officer, laboratory manager, quality manager, scientist, technician, information and communication technology personnel, human resources officer, security personnel) to ensure a comprehensive view of the laboratory biosecurity management and implementation.

You can start at any pillar of your choice and answer the questions on that particular subject, and then work through all the pillars. Read and understand the questions before going any further.

1. Please fill in the following questionnaire on the basis of the facts of your facility.

2. Please answer all questions. Choose your response between "Yes", "No", "Not Applicable (NA)" or "In Progress". You can also list down your observations or findings in the comments columns.

The results of the questionnaire will provide you a picture of the current state of affairs in your organisation and what still needs to be done. The ultimate objective of this checklist is to help organisations to improve biosecurity in their respective organisation.

NATIONAL LABORATORY BIOSECURITY ASSESSMENT AND MONITORING CHECKLIST

DETAILS OF THE INSTITUTION

Institution	:	
Name of the facility	:	
Type of facility	:	
Location/Address	:	
Type of Valuable Biological Material(s) (VBM)	:	
Person in charge	:	
Email	:	
Telephone/Mobile number	:	

A. MANAGEMENT

No.	Item	Yes	No	NA	In Progress	Comments
1.	Does the management assign specific roles and responsibility as specified in the CEN Workshop Agreement (CWA) 15793 document? *(The management system formally specifies the function of each personnel within the organisation*)					
2.	Does the organisation have a policy on biorisk management (safety and security) that has been developed, authorised and signed by the organisation's top management? *(Having a formally approved policy on biosecurity by the highest management of the organisation*)					
3.	Is the organisation's top management actively involved in the policy on biosecurity? *(Actively involves and updated in the development and progression of the organisation's policy on biosecurity)*					
4.	Is the policy on biosecurity revised, periodically, on the basis of experiences and risk assessments? *(Assessments are important to assess the adequacy of existing procedures. Where necessary, procedures may be revised, following such an assessment*)					
5.	Is dedicated budget/resources allocated for the management of biosecurity?					

No.	Item	Yes	No	NA	In Progress	Comments
6.	Is the budget adequate to execute planned/projected projects/activities/trainings on biosecurity? *(Demonstrates the track record/accounting evidence (both financial and non-financial) that sufficiently supports the biosecurity related activities within the organisation)*					
7.	Does the organisation have a system in place to monitor unauthorised personnel to allow them to conduct routine non-laboratory functions (cleaning, maintenance, repairs, etc.)? *(Having a formal procedure/guideline to ensure that the organisation's biosecurity status remains intact in the presence of outsiders)*					
8.	Does the organisation have a system to conduct and review the biosecurity assessments? *(The organisation works toward having person(s) with relevant knowledge and experiences to perform biosecurity assessment, otherwise having an external qualified assessor to validate the organisation's biosecurity assessment activity)*					
9.	Has the organisation assigned personnel to oversee the implementation of biosecurity measures? *(The organisation formally appoints a personnel and provides support for the appointed person to be formally trained/certified in the area of biosecurity)*					
10.	Does the organisation conduct periodical risk assessments on Dual Use? *(Dual Use could refer to the potential misuse of biological agents, equipment, research, publication, methods, etc.)*					

No.	Item	Yes	No	NA	In Progress	Comments
11.	Does the organisation have a systematic communication mechanism in place to quickly disseminate biosecurity information to those who manage, perform and verify work associated with the control of biological agents and toxins? *(Making use of information technology to ensure that all stakeholders receive the required information on biosecurity)*					
12.	Is adherence to the procedures and rules of conduct being monitored? *(This concerns compliance with biosecurity agreements on individual staff level e.g. the judicious use of passwords)*					
13.	Does the organisation have an evaluated list of certified vendors/buyers for biological substances? *(Having a formal procedure to select trusted vendors/buyers)*					

B. BIOSECURITY AWARENESS

No.	Item	Yes	No	NA	In Progress	Comments
1.	Does the organisation have at least an annual biosecurity awareness seminar/talk/day/etc. for all personnel working in laboratory? *(Awareness programmes that target personnel who are not directly involved in biosecurity implementation) (Please attach training/awareness programmes records)*					
	a) Permanent/fulltime personnel					
	b) Contract/part-time personnel					
	c) Intermittent personnel (vendors, contractors, maintenance, cleaners, etc.)					
2.	Does the organisation have an entry-level biosecurity orientation programme for the new personnel, which emphasises on the eight pillars of biosecurity, their roles and responsibilities? *(Orientation programme regarding biosecurity procedures and biosecurity codes which raise biosecurity awareness and involvement of personnel and their roles and responsibilities)*					
3.	Does the organisation have a continuous training programme planned for all the personnel involved in implementing biosecurity, including response to biosecurity breach? *(Organisation should provide scheduled advanced training for those who are responsible in implementing biosecurity) (Please attach training records)*					

No.	Item	Yes	No	NA	In Progress	Comments
4.	Is dual use being incorporated in the training and awareness programmes? *(Should incorporate dual use and potential dual use in training and awareness programmes)*					
5.	Are personnel aware of reporting mechanism of any biosecurity breach and that the anonymity of whistle-blower is protected? *(This would include means to prevent and address retaliation - Whistle-blower Protection Act 2010)*					
6.	Does the institutional biosecurity programme transcend through the organisation and run by knowledgeable/experienced personnel?					
7.	Is the top management aware of the significance of biosecurity programme and their responsibilities? *(This may be reflected by appointment of dedicated personnel by top management, through whom the management is updated of the biosecurity programme)*					
8.	Are personnel aware of the existence of response mechanism and their responsibilities in the event of any biosecurity breach? *(Personnel working in the laboratory need to be aware of the required course of action and must act accordingly in the event of biosecurity breach)*					
9.	Are personnel aware of their responsibilities regarding biosecurity and how responsibilities are assigned? *(Personnel working in the laboratory must be made aware of where their responsibilities lie within their organisation, as well as who to address when they have any questions about biosecurity)*					

C. PHYSICAL SECURITY

No.	Item	Yes	No	NA	In Progress	Comments
1.	Do different areas of the facility have different levels of security? *(Security level may depend on criticality of the area; e.g. administrative areas, laboratory areas, short and long term storage areas, security operations centre, sensitive information storage areas, containment laboratories)*					
2.	Does the management enforce access control policy? *(Selective restriction of personnel to secured areas in the facility or access to biological agents/resources. The act of accessing may mean entering, consuming or using)*					
3.	Are the access controls monitored for each secured area?					
4.	Does the organisation have closed-circuit televisions (CCTVs) in the premise?					
	a) If yes, are these CCTVs strategically located?					
	b) Are these CCTVs monitored? *(Monitoring by means of reviewing and/reported by person in-charge)*					
5.	Is there an intrusion detection system to detect unauthorised entry to the facility and biological agents' storage areas?					
6.	Is there camera coverage for all exterior laboratory building entrances?					

No.	Item	Yes	No	NA	In Progress	Comments
7.	Is there sufficient perimeter lighting for the facility?					
8.	Is there a vehicle screening practice in place?					
9.	Is an identification card or badge used to identify all personnel and visitors within the confines of the controlled areas?					
10.	Are all personnel and visitors required to wear the security identification badge while on premises?					
11.	Is there a visitor escort procedure established for gazetted secured areas?					
12.	Do the laboratory doors have locks?					
13.	Are the laboratory doors self-closing?					
14.	Are locks and keys to all buildings and entrances supervised and controlled by a key control official?					
15.	Are keys issued only to authorised personnel?					
16.	Are valuable biological materials (VBM) stored in secured locations? *(VBM are determined by institution/organisation)*					
17.	Is the entrance to the secured area, or storage location, secured by a combination of methods? *(These methods may consist of: Something you have (key), something you know (PIN code), something you are (biometrics)*					
	a) Are the mechanisms sufficient to secure the area?					

D. ACCOUNTABILITY FOR MATERIALS

No.	Item	Yes	No	NA	In Progress	Comments
1.	Does the organisation have a policy on the inventory management of valuable biological materials (VBM)? *(VBM may include biological agents such as pathogens, toxins, cells, vaccine strains and other materials valuable to the organisation)*					
2.	Does the organisation have policy on the transfer of VBM?					
3.	Does the organisation have biosecurity procedures in place to prevent deliberate dispersion of biological agents?					
4.	Is there a person assigned, responsible for the registration and the active management of VBM in order to safeguard the control of these materials?					
5.	Does the organisation maintain and update inventory records based on the following activities:					
	a) Purchase of VMBs?					
	b) Receive/arrival of VBM? *(Name of sender, receiver, the packaging integrity, etc.)*					
	c) Transfer of biological agents?					
	d) Destruction/disposal of biological agents (including verification that materials have been autoclaved)?					

No.	Item	Yes	No	NA	In Progress	Comments
6.	Does the inventory system in the organisation include detailed information regarding the location of the biological agents? *(This question emphasises on the information security of the material inventory)*					
7.	Does the organisation conduct periodic reviews/crosschecks of biological agents' inventory (including storage and location)?					
	a) Are there proofs of records (of the periodic reviews/ crosschecks)?					
8.	In the event of unusual or suspicious event involving activities in Questions 5a-5d and 7, does the organisation have a system that triggers investigation (including record discrepancies, missing biological agents)?					
9.	Are there biohazard signage at the entrance of laboratories and storage spaces to indicate presence of biological agents without revealing the organisms? *(From the perspective of biosafety, it is necessary to provide clear indication of the presence of specifically high-risk biological agents. However, from a biosecurity perspective, detailed information should only be available to authorised personnel)*					
10.	Are inventory storage locations minimised and adequate protection is provided so that only authorised personnel have access?					
11.	Are the VBM at the organisation limited to a certain quantity? *(Organisations should not have an oversupply of materials in stock)*					

E. INFORMATION SECURITY

No.	Item	Yes	No	NA	In Progress	Comments
1.	Has the organisation formulated and implemented a policy on information security? *(The policy document describes the manner in which confidential information is handled within the organisation and it is the basis of operational information security)*					
2.	Does the organisation use a classification system to determine sensitive information? *(Sensitive information refers to information that should not be disclosed such as research data, personnel identifying information, location and type of biological agents, etc. The organisation must describe how to determine sensitive information and how this type of information must be handled in order to prevent disclosure)*					
3.	Does the organisation have policy and procedures on individual authorisations regarding access to sensitive/confidential information? *(Access to sensitive/confidential data should be granted only to personnel who have a demonstrable need to access it and with appropriate personnel security control. Graded access level may be assigned to the information after risk assessment has been carried out and the necessary steps to mitigate the risks identified)*					
4.	Do all personnel know and understand the procedures regarding access to sensitive/confidential information?					

No.	Item	Yes	No	NA	In Progress	Comments
5.	Has the organisation assigned authorised personnel, responsible for information security? *(Organisations are required to have an overview/list that contains the names of appointed personnel authorised to access and manage this information)*					
6.	Is sensitive/confidential information, including paper information, stored in a physically secured place?					
7.	Are computers that store sensitive/confidential information password protected?					
8.	Does the organisation install relevant security software to the computers that store sensitive/confidential information?					
9.	Is there information back-up system in place for sensitive/confidential information?					
10.	Does the organisation practice protected electronic data transfer? *(Examples: using dedicated email, encrypted email, the use of secure USB flash drives, etc.)*					
11.	Are there procedures on emergency response in the event of breach of information security? *(The emergency response procedures describe how the organisation prepares for and deals with breach of information security to secure and limit the impact)*					

No.	Item	Yes	No	NA	In Progress	Comments
12.	Has the organisation implemented administrative control measures with regards to the exchange of sensitive information					
	a) within the organisation?					
	b) between different organisations?					
13.	Are guidelines available on publication that has potential issue of dual use? *(Dual use refers to biological agents, technology or knowledge, which can be used for 'good' purposes but could also be misused)*					

F. TRANSPORT SECURITY

No.	Item	Yes	No	NA	In Progress	Comments
1.	Are guidelines, SOPs or working instructions related to transport of valuable biological materials (VBM) available					
	a) within the organisation?					
	b) between different organisations?					
2.	Are personnel responsible for transporting the VBM trained in specific requirements and procedures for the transport of these materials? *(Personnel are trained in the requirements for packaging and transport of the biological agents (e.g. infectious or genetically modified micro-organisms, diagnostic samples) according to regulations)*					
3.	Does the selected transport company comply with legislations? *(Organisations need to ensure that the transport companies chosen to transport biological agents comply with the necessary legislations i.e. International Air Transportation Association (IATA) and Standard Operating Procedure for Transport of Biological Specimens in Malaysia (2012.)*					
4.	Does the organisation have a pre-selection procedure for the transport companies they intend to use for transportation of the VBM?					

No.	Item	Yes	No	NA	In Progress	Comments
5.	Does the organisation enforce chain of custody? *(The chain of custody process documents that an accountable individual has control over the integrity of the packaged material, and that secure receipt of the material has occurred at the appropriate facility location. The documentation includes the name and quantity of material being moved, the shipping and consignee contact information (or laboratory contact information as applicable), and time, date and signatures of every individual who assumes control of the material en route (e.g. those who initiate delivery, package, or relinquish custody)*					
6.	Is the track and trace system for the transportation of biological samples available?					
7.	Is there a Material Transfer Agreement (MTA) between the organisation and the sender/recipient of the VBM? *(An example of such an agreement would be that the recipient reports the actual receipt of said materials)*					
8.	Does the organisation ensure that the recipient institution has the appropriate level of biorisk management to receive the sample? *(In relations whereby biological substances are exchanged or sent to be tested by other organisations, it is important that these organisations have the appropriate or comparable biorisk management system in place)*					

No.	Item	Yes	No	NA	In Progress	Comments
9.	Does the organisation conduct risk assessment for each transportation type used? *(Results from the risk assessment may be used to implement certain measures that would reduce any risks)*					
10.	Is the emergency response plan available for the possibility of packages being lost during transportation? *(The emergency response plan describes how the organisation prepares for emergencies that might occur during transportation)*					

G. PERSONNEL RELIABILITY

No.	Item	Yes	No	NA	In Progress	Comments
1.	Does the organisation have a personnel assessment in place?					
2.	Are new recruits in the organisation subjected to a formal background screening process including credentials, skills, personnel traits and relevant background check based on risk assessment? *(Screening may include social and criminal background checks and financial probity)*					
3.	Are background checks conducted on existing personnel on periodical basis?					
4.	Were mental health assessments/psychological assessments conducted prior to employment or in interval time of employment?					
5.	Does the organisation have policy and guideline on visiting personnel (students, contractors, visitors, clients, temporary workers, etc.) regarding security clearance to access the facility?					
6.	Does the organisation have an up-to-date list of personnel with authorised access to the facility and biological agents?					
	a) Permanent/fulltime personnel					
	b) Contract/part-time personnel					
	c) Intermittent personnel (vendors, contractors, maintenance, cleaners, etc.)					

No.	Item	Yes	No	NA	In Progress	Comments
7.	Does the organisation have policy and guideline in place for personnel to report or register unusual behaviour in co-workers or visitors? *(Unusual behaviour is behaviour that is inconsistent with that expected of a particular person)*					
8.	Does the organisation have a system in place in terms of assessment if existing personnel are transferred to areas where there may be an increased risk profile? *(Assessment shall include mental health and psychological status, financial status, political inclination, criminal record, etc.)*					
9.	Does the organisation have a system in place for the removal and exclusion of personnel (both temporary and, if appropriate, permanent) from the access to the facility or access to the biological agents where it deems necessary through risk assessment?					
10.	Does the organisation have SOPs or guidelines to monitor employees working outside regular hours?					

H. EMERGENCY RESPONSE

No.	Item	Yes	No	NA	In Progress	Comments
1.	Does the organisation have emergency response plan to effectively respond and control biological emergencies or a biosecurity breach (e.g. theft, intentional release, sabotage, etc.)? *(The emergency response plan describes how the organisation prepares for emergencies/disasters and how various types of biological emergencies including biosecurity breach must be dealt with to confine the biological agents and limiting their impact, including reporting biosecurity emergencies and/or breach to the relevant authorities and/or first responders (e.g. police, fire department, medical provider, etc.)*					
2.	Does the emergency response plan contain tasks, responsibilities and authorisations for response and recovery, including investigation of biological incidents/emergencies? *(The emergency response plan should indicate who to alert/report to in case of an emergency/biosecurity breach, and how operational responsibilities have been assigned)*					
3.	Does the organisation have a contingency plan in place to guarantee the continuation of day-to-day operations with a sufficiently high level of security? *(The contingency plan enables the organisation to continue, repair or restore its main activities in case of a breakdown in ICT and/or machinery, and/or power failure)*					

No.	Item	Yes	No	NA	In Progress	Comments
4.	Does the organisation have arrangements/collaboration protocols with relevant parties (e.g. fire department, police, medical provider, local council) in the event of biological emergencies/biosecurity breach? *(This concerns arrangements regarding the biosecurity risks made with local council, police, fire department, emergency medical assistance and other national authorities)*					
5.	Does the organisation organise emergency drills or exercises (at least annually) that also look at biosecurity risks to determine that personnel can respond adequately/competently to emergencies and other biosecurity situations according to plans and/or expectations? *(These drills are management and/or operational exercises (e.g. tabletop exercise, field exercise) that are part of the policy on education, awareness, training, and drills)*					
6.	Does the organisation establish procedures to correct situations where biosecurity is compromised? *(These incidents could be evaluated and registered, and the root cause could be investigated)*					
7.	Does the organisation establish preventive actions or revise procedures to make sure that situations where biosecurity were compromised will not recur? *(The procedure is taken in response to the results of incident investigations, exercises, drills, or other reviews, and includes determining the potential non-conformities and their causes)*					

Science and Technology Research Institute for Defence (STRIDE)
Ministry of Defence Malaysia
Kompleks Induk STRIDE, Taman Bukit Mewah Fasa 9
43000 Kajang Selangor

Tel: (603) 8732 4400

Website address: http://stride.gov.my/

ISBN 978-967-16592-1-2