MIRRI IS21
IMPLEMENTATION AND SUSTAINABILITY FOR THE 21ST CENTURY
MICROBIAL RESOURCE RESEARCH INFRASTRUCTURE

D3.6

Guidance document on implementing biorisk management in MIRRI mBRCs

The project “Implementation & Sustainability of Microbial Resource Research Infrastructure for 21st Century” (IS_MIRRI21) has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement nº 871129. This document reflects only the author’s view and the European Commission is not responsible for any use that may be made of the information it contains.

Project number:	871129
Project acronym:	IS_MIRRI21
Project title:	Implementation & Sustainability of Microbial Resource Research Infrastructure for XXI Century
Start date of the project:	1st February 2020
Duration:	42 Months
Programme:	H2020/Research and Innovation Actions: INFRADEV-03-2019

Deliverable type:	Report
Deliverable reference number:	D3.6
Work package:	WP3
Due date:	31 July 2023
Actual submission date:	16 May 2023

Responsible organisation:	UMINHO		
Editor:	Armando Venâncio, Marizeth Groenewald & Gerard Verkley		
Version:	**Revised by:**	**Date:**	**Notes:**
V1.0	Marizeth Groenewald & experts	12-04-2023	1st Draft
V1.1	WP3 Beneficiaries	21-04-2023	Contributions
V1.2	Gerard Verkley	21-04-2023	Revised version
V1.3	Bassem Kheireddine	23-04-2023	Revised version
V1.4	Pierre Becker	26-04-2023	Reviewer 1
V1.5	Justyna Nasilowska	01-05-2023	Reviewer 2
V2.0	Nelson Lima	16-05-2023	Submission

Abstract:	This guidance document aims to support MIRRI mBRCs on implementing, improving, and maintaining biosecurity procedures to prevent the loss, theft, or misuse, of biological microorganisms that are stored, studied, transferred and/or supplied by the mBRC.
Keywords:	Guidance – Biorisk– mBRCs – Biosecurity – Biosafety

Dissemination level:	Public	X
	Confidential (for the Consortium and EU Commission Services only)	

Abstract

This guidance document aims to support MIRRI mBRCs on implementing, improving, and maintaining biosecurity procedures to prevent the loss, theft, or misuse, of biological microorganisms that are stored, studied, transferred and/or supplied by the mBRC.

Contents

1. Introduction

1. Introduction

Various MIRRI microbial Biological Resource Centers (mBRCs) are entrusted maintaining and exchanging of hazardous biological material. Therefore, this guidance document on implementing biorisk management is provided to ensure the proper maintenance and provision of their biological resources. MIRRI wants to promote collaboration and assist stakeholders in managing risks associated with biological material, creating a forum of experts where scientists, policy makers and mBRC managers can share concerns and good practices. This guidance document aims to support MIRRI mBRCs on implementing, improving and maintaining biosecurity procedures to prevent the loss, theft, or misuse, of biological microorganisms that are stored, studied, transferred and/or supplied by the mBRC.

Along with these recommendations, MIRRI mBRCs are required to operate in accordance with applicable national, European, and international legislation and to follow the Biosecurity code of conduct for BRCs as well as the principles of the OECD Best Practice guidelines on biosecurity for BRCs (links provided in the appendix).

2. Biorisk management in MIRRI mBRCs

2. General principles for biorisk management at mBRCs

To implement biorisk management procedures it is essential to define first the concepts of Biosecurity and Biosafety.

Biosecurity refers to institutional and personal security measures and procedures to prevent the loss, theft, diversion, and intentional release of hazardous biological resources that are maintained, transferred and/or supplied; whereas biosafety aims at protecting the worker handling hazardous material, society (in general) and the environment from accidental exposure to biological agents. Therefore, it is considered that biosecurity and biosafety are complementary and with time biosecurity has become associated with biosafety to form the contemporary approach of biorisk management, which is the process of evaluating policy alternatives, considering risk assessment and other tools relevant to biosecurity, and selecting appropriate prevention and control actions.

To properly undertake biorisk management, the mBRC shall assign adequate resources and responsibility to guarantee compliance with legal requirements by adopting published biosecurity guidelines, best practices, and codes of conduct (see section 12 with references). For this, it should appoint a person responsible for the biorisk management of the mBRC (biorisk management officer) as well as his/her proxy. In large institutes, a team of responsible persons, the biorisk management committee, is recommended to, carry out this task. These persons should be competent to integrate biorisk management throughout the mBRC and ensure that it is well implemented and continuously improved, following the recommendations below.

3. Assessing biosecurity risks – virulence and risk of potential misuse

Biorisk assessment evaluates the potential harm to humans, animals, plants and/or the environment arising from a biological microorganism. Such harm can result from unintentional exposure, accidental release, or loss, theft, misuse, diversion, unauthorized access, or intentional unauthorized release. Pathogenic microorganisms can be classified in terms of their virulence and transmissibility, the severity of the disease that they can cause, and the availability of countermeasures.

To evaluate the virulence several factors can be considered, including:

- the smallest infective dosage that is needed to cause harm
- the pathogenicity level; disease-causing ability
- the host range and host specificity
- whether or not it is lethal to its host and host population (in the latter case the percentage of lethality). If not lethal, the severity of the disease should be considered, meaning for instance the disability that it causes to its host, or the associated health costs

- if there are effective treatments available
- whether it can be (easily or not) transmitted from one host to another – among individuals of the same host species, or between species (from animals to humans etc.)
- the way the disease is transmitted: airborne, body contact or via body fluids, sexually transmitted disease, via vectors, etc.

Factors that can impact the risk of misuse of pathogenic microorganisms include:

- availability of the strain from natural sources, or other facilities.
- ease of multiplication
- ease and effectiveness of dispersal
- agent stability in the environment
- level of skill and knowledge needed to use the organism to cause harm (e.g. develop a weapon)
- availability of countermeasures, prophylactic measures, either physical barriers or bio-barriers (vaccines, immune boosters, …)
- non-compliance with the operating instructions, inattention, staff carelessness

For the evaluation of Genetically Modified Organisms (GMOs), the potential pathogenicity/virulence of both the host and the donor shall be considered, to determine the potential risk of the new construct (see Directive 2009/41/EC Annex III).

Indicative lists of regulated organisms (see references and links in section 12) include:

- The Association for biosafety and biosecurity (ABSA International) Risk Group Database
- The Australia group Common Control Lists: list of plant pathogens listed as dual-use organisms
- The UK Plant Health Risk Register (Defra)
- The European and Mediterranean Plant Protection Organization (EPPO) Global Database
- European Implementing Regulation 2019/2072 about protective measures against pests of plants
- Regulation (EU) 2021/821 about the EU's export control regime of dual-use items
- Directive 2000/54/EC on the protection of workers from risks related to exposure to biological agents at work
- Laboratory biosafety manual, WHO

Most of these lists classify the microorganisms according to Risk Groups (RG, evaluating the risk of infection) and Biosafety Levels (BSL) or containment levels; consisting of a set of protective and containment measures to safely handle the microorganisms (including GMOs) and avoid adverse effects in humans, animals, plants, and the environment. It is crucial to remember that the RG for some of the organisms listed on several of these lists may differ among countries,

even those within Europe. Therefore, it is important always to consolidate GR listings of the country in scope.

The safe handling of pathogenic and/or genetically modified microorganisms is regulated by Directive 2000/54/EC on the protection of workers from risks related to exposure to biological agents at work and Directive 2009/41/EC on the contained use of genetically modified micro-organisms. The mBRC should identify the biological material on at least the species level, unless otherwise specified in the regulation lists, and gather information at the species or the strain level about the potential risks from additional sources (e.g., publications, strain deposit form). The biorisk assessment shall be performed on new acquisitions and on current collections, including a regular review (e.g., quarterly) of any impactful legislation or regulatory requirements changes. The risk evaluation shall be done following precautionary principles. The mBRC shall maintain a detailed and up-to-date inventory of the different biological materials kept in the collection. When conducting a biosecurity risk assessment, the following aspects shall be considered:

- Actors that might wish to misuse pathogenic microorganisms.
- Intent: e.g., theft, intentional release, development of biological weapons.
- Asset: which pathogenic microorganisms could be attractive to threat actors.
- Likelihood: how likely is that threat actors would act upon their intent.
- Consequence: what the consequences of such actions could be.

To prevent the risk of biological misuse and weapon development, states must implement export controls on pathogenic microorganisms of biosecurity concern and the equipment required for their use and manipulation. Relevant international and EU instruments include the Australia Group Common Control Lists: a list of plant pathogens listed as dual-use organisms and Regulation (EU) 2021/821 about the EU's export control regime of dual-use items. In addition, facilities and organisations handling pathogenic microorganisms must have appropriate institutional biosecurity policies, procedures, and measures to manage the risk of misuse. This document addresses the key elements of a biosecurity management system.

Considering these aspects, the Biosecurity Risk Levels for microorganisms are generally classified as follows:

Negligible or Low risk – generally RG-1, BSL-1 organisms, and containment level 1 of GMOs.

Moderate risk – generally RG-2, BSL-2 organisms, and containment level 2 of GMOs

High-risk – generally RG-3/4, BSL-3/4 organisms, listed Dual-use and quarantine organisms, and containment level 3/4 of GMOs

The mBRC shall maintain a detailed and up-to-date inventory of the biological materials kept at the collection, including their Biosecurity Risk Levels.

The biorisk assessment shall be performed on new acquisitions and current holdings by a competent permanent employee of the mBRC, preferably from the curation team or an appointed biosafety officer or biorisk manager. If there is doubt as to whether a particular factor of a biological

material should be characterized as high or moderate the evaluation shall follow a precautionary principle, assigning the highest necessary level. It is recommended that the person in charge of this task is aware of new developments on risk assessment of materials and seeks advice from researchers, expert networks such as the MIRRI biosecurity expert cluster, or individual experts on biosecurity.

4. Physical security and access control

mBRCs should adapt their physical facility to reflect three barriers of secure areas. This includes the general area, the moderate restricted area, and the high restricted area.

General areas refer to areas to which all employees and escorted visitors have access, without physical barriers. Work on microorganisms is not permitted in these locations. Depending on the infrastructure some mBRCs need a general area.

Moderate restricted areas have physical security barriers (e.g., manual keys, electronic key cards, presentation of personal ID badges to security) for access control, avoiding unauthorised access. They are accessible to only those employees and visitors with appropriate authorisation, e.g., 1) short term guests (external maintenance/cleaning staff and day visitors) which shall be accompanied always by authorized personnel and 2) long term employees and guests that have personalized means of access. It is recommended that mBRCs have all their facilities where cultures are handled at least inside the moderate restricted areas.

High restricted areas should have an additional barrier of security and access control by means of electronic key cards or biometric security systems (palm reader or iris scan) (preferred) and/or physical key's that are only accessible to authorised personnel. Windows, ventilation, and other spaces should be constructed in such a way to prevent unauthorised access. The use of camera detection/alarm systems is recommended. Institute personnel and escorted visitors with access to restricted areas should be minimal and appropriate to need. If personalised (key) cards or badges are used it is recommended that they clearly display the level of security clearance and they shall under no circumstances be shared with any other person, even with authorised employees. It is recommended that a logbook or a registration system is in place to keep track of people entering these secure areas, including names and affiliation of maintenance or cleaning personnel.

All actively growing high risk cultures are only handled and stored within the high restricted areas. There should be no exceptions to this rule.

5. Security management of personnel and visitors

BRCs should establish a system of different levels of security controls for employees and visitors. Personnel shall be trained in basic security issues, and understand that personalised

(electronic) access keys/cards and log-in credentials for access to data and applications shall never be provided to others.

An authorised employee should always escort day or short-term visitors into the restricted area(s). Engineering maintenance and cleaning personnel should only be authorised to access areas appropriate to their activity. Short-term visitors should be made recognisable with a visitor's badge and their visit shall be recorded using a logbook or a similar system. They shall not have access to highly restricted areas unless authorised by the biorisk manager (e.g. for maintenance/cleaning activities).

The primary screening of new employees and long-term temporary visitors (e.g., interns, visiting researchers and students), should be done by a responsible person (e.g., the biorisk manager, the Principal Investigator (PI) of the group or the human resources department) in collaboration with national authorities if applicable. They shall be trained in biosafety and biosecurity practices within the mBRC, and they should work closely with an authorised employee during an interim period to evaluate their competence. Once they are familiarised with the layout and work procedures at the mBRC and have shown to be competent to carry out assigned tasks, security access to restricted areas may be granted.

In high-risk areas workers will not be allowed to work without direct or remote supervision for his/her personal safety (intervention in case of incident) and for the safety of the laboratory (malicious intent). Workers should undergo special training required to work in high-risk areas.

Authorisation to work after hours shall be justified and granted only to permanent/long-term employees and escorted visitors. Personalised access clearance to high restricted areas and high-risk material or data should be well monitored, documented, and approved by the biorisk manager. Any mode of access to restricted areas and data should be disabled on the day the contract of employment/visit ends.

6. Incident response plan

mBRCs should devise and adopt an incident response plan for recording, reporting, and investigating security breaches and the immediate actions to be taken, guided by applicable national and international laws. The detailed information in the incident response plan that are important for the staff members (including non-technical personnel) shall be made available to them. All staff members shall be trained in these actions and encouraged to report any finding or suspicion of misuse of biological material, information, or technology directly to the competent persons to take further actions.

The plan shall identify the internal person(s) that should be contacted after a possible security breach, as well as the list of external parties and authorities to be contacted when appropriate. The internally responsible person(s) should retrieve and compile information to evaluate the risks and take necessary measures to address the security breach. Depending on the type of risk (risk to human, animal, plant and/or other environmental/societal area) and the severity, external

parties/authorities (local, regional and/or national) shall be informed to take further action. The mBRC shall keep an up-to-date list of people who have legitimate access to high-risk material or data, and an inventory of requests received for high-risk organisms, and they shall be made available upon request after a security breach. The incident response plan should be tested regularly by initiating practice exercises to emphasise possible weak points.

The contingency plan should include the ability to deal with a power outage.

The contingency plan shall be available to internal and external emergency response teams (e.g., company and municipal fire departments).

7. Community training and development of a biosecurity-conscious culture

All employees (including non-technical staff) and long-term visitors should be trained and regularly updated (e.g., annually) on biorisk management procedures of the facility, including information about the Incidence response plan (see also section 6, Incident response plan). The training will be compulsory for all employees and long-term visitors working with high-risk organisms and keeping an attendance list of these sessions is recommended. In addition, employees and visitors having access to high-risk information should be aware that their source of knowledge could present a security risk.

Specific external training courses might be compulsory for employees and visitors carrying out tasks that require a certificate or additional training to ensure compliance with laws and regulations, e.g., staff involved in the distribution of microorganisms or involved in the Biorisk management.

All technical employees must be informed about changes in Biosecurity requirements or changes in the lists of potential high-risk organisms, especially where these changes have an impact on the daily practices to handle these microorganisms.

The mBRC shall promote the creation of a biosecurity conscious culture in the community and transparently conduct its activities, striving to build trust in its relations with the local community.

In addition, mBRCs are frequently part of a host institute and share facilities, including e.g., BSL-3, with other laboratories. Biorisk management is thus also organized at the level of the host institute. Good collaboration and communication between the mBRC and the biorisk management team/responsible of the host institute is therefore essential.

8. Material control and accountability

It is highly recommended that mBRCs implement a stock management system (e.g., databases or spreadsheets) for all the material held at the collection. The system should include an up-to-date inventory of all microorganisms, their biorisk properties, the number of vials available and their location, the internal and external transfers (including the date of transfer and information on the end-users/responsible person) and remarks on any deviation in the unit numbers due to

general collection activities or unforeseen situations. If possible, all order histories, including letters of orders, MTAs or permits and regulatory documents should be kept indefinitely, or for a period at least by applicable law or institutional management guidelines. Besides, the mBRC should make inventories on the number of units available of all the material. For the high-risk organisms, the stock control is mandatory, and the frequency of the inventories shall be at least once a year and include a revision of the data linked to the microorganism, to ensure accuracy and up-to-date information.

It is advised that employees and visitors handling high-risk material sign, prior to use, a biosecurity acceptance of responsibility form. This form shall contain details about the stock to be used, the procedures/protocols to be carried out and the location of the material at all times. At the end of the work the users should report back to the biorisk manager that the high-risk material in their possession has been destroyed (e.g., autoclaved).

9. Data security

The mBRC should have a system to record and back-up all relevant information of the material (e.g., isolation and deposit information, cultivation methods, sequence data, stock availability and transfers). It should undertake a risk assessment on the data associated with the material, especially data linked to high or moderate risk microorganisms, and develop a policy about which type of data should be permanently excluded from the public domain, and the level of clearance that needs to be assigned to different data for (internal) access by staff. Access to highly risk-sensitive information, such as data on GMOs having increased biorisk properties or the specific location of high-risk organisms shall be granted by the biorisk manager on a need-to-know basis and restricted to personnel with security clearance to access the physical or biological material. Employees with access to these data are not allowed to give their login details to anyone. Paper copies of this type of information should be locked away, with physical keys only accessible to authorised personnel and when no longer used, it must be destroyed within a paper shredder or by alternative means.

10. Supply and transport of high-risk material

a. internal to the mBRC

Requests for strains for research purposes within the mBRC, should be documented as described in section 8, Material control and accountability, and the supply chain should be traceable. All high-risk material should be secured and handled in the highly restricted area(s) and designated laboratories. Exceptions (e.g., the need for special equipment or incubators outside the high-risk area) shall be carefully evaluated and authorised by the biorisk manager and should be done in at least moderate restricted areas within locked incubators or doors. At no time should the storage/incubation location of the material be accessible by unauthorised persons.

High-risk material must be physically contained in closable leak-proof boxes labelled with the biohazard sign when transported between laboratories and incubation rooms, and preferably respecting the double barrier principle (double containers).

b. external to the mBRC

Documentation of requests should follow the description section 8, Material control and accountability, and the supply chain should always be traceable. For requests of moderate and high-risk organisms it should be clear to the end users that appropriate biosafety and biosecurity measures are needed to handle and store the requested material. Material should never be sent to private addresses and end-users should sign an acceptance of responsibility declaration acknowledging compliance with applicable biosafety and biosecurity regulations. All this should be mandatory for the shipment of moderate and high-risk organisms. Screening of recipients of high-risk materials in coordination with the relevant authorities and parties is recommended. If desired, certificates, that can act as proof of compliance to Biosecurity standards, can be requested from the recipient. For the high-risk microorganisms, it might be mandatory to ask a certificate proving that the recipient has access to facilities for their manipulation. Refused requests and the reason for rejection for high-risk organisms should be documented. Shipment of accepted requests should be monitored until notification of arrival to the final user. It is highly recommended that all documents related to the supply of material outside of the facility (request of order, MTAs, regulatory documents etc.) should be stored indefinitely, or according to the host institute's archiving rules.

mBRCs should follow all the applicable national and international regulations, (see relevant references in section 12) to ensure safe and secure packaging and transportation of all biological material and to guarantee that all regulations on export control are met. Employees trained in such regulations shall be responsible for the distribution of this biological material outside of the mBRC. For high-risk organisms, select transporters allowed to handle this type of material.

11. Auditing aspects of biorisk management process

mBRCs should establish a timetable for internal biosecurity audits covering at least two-year periods and based on risk assessment to prioritise an audit. Such audits should aim to determine the correct implementation of biorisk management and adopt available guidelines, best practices, and codes of conduct to ensure internal compliance with biosecurity.

The audits should be documented and done by the biorisk manager with the help of additional trained employees. They should include all aspects specified above: physical and data security, security management of visitors and employees, incident response plan, developing a biosecurity-conscious culture among employees, material accountability, supply, and material transport.

Random sampling shall be made on cultures and data of high-biosecurity risk separately. Some examples of elements to list in the internal audit include:

1) biorisk assessment of (high-risk) material: it should be up-to-date, and information correctly recorded in the database;
2) physical inspection of facilities: pay special attention to the security access of high and moderate restricted areas in the building;
3) accessibility of secure areas: ensure that only authorised persons have access;
4) inspection of the facilities: ensure that the materials are stored and handled within the appropriate secure area;
5) accessibility to high-risk data: ensure that it is appropriately restricted (and backed-up on a remote server, and that only authorised persons have access;
6) personnel training: check that relevant persons attend regular (at least yearly) biosecurity training and revise that the information provided is up to date;
7) personnel training: audit training records to ensure professional competence required is reflected in the record. Also check that technical competency “refresher training” is completed;
8) material supply: check conformance with the procedures;
9) documented information: responsible persons are supplied with the most up-to-date lists of restricted organisms and working procedures that are version controlled;
10) corrective actions: evaluate the measures taken after a security breach (if any) or incidence of a non-conforming product.

3. References

12. References to relevant guidelines, agreements, and regulations

1. General biorisk guidelines:

1. WHO guidelines
https://www.who.int/publications/i/item/9789240011311 (accessed on 12 April 2023)

2. OECD best practice guidelines on biosecurity for BRCs
https://www.oecd.org/sti/emerging-tech/38778261.pdf (accessed on 12 April 2023)

3. A Code of Conduct for Biosecurity (2008) Royal Netherlands Academy of Arts and Sciences Report by the Biosecurity Working Group. Amsterdam,

ISBN 978-90-6984-535-7

4. Code of Conduct on Biosecurity for Biological Resource Centres (BRCs) Procedural implementation (2013)
doi:10.1099/ijs.0.051961-0

2. Guidelines for biosecurity risk group assessment:

1. ABSA for biosafety and biosecurity
https://my.absa.org/tiki-index.php?page=Riskgroups (accessed on 12 April 2023)
2. Australia group
https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/human_animal_pathogens.html (accessed on 12 April 2023)
3. Defra
https://planthealthportal.defra.gov.uk/ (accessed on 12 April 2023)
4. EPPO
https://gd.eppo.int/ (accessed on 12 April 2023) and
https://www.eppo.int/media/uploaded_images/RESOURCES/eppo_standards/pm1/pm1-002-31-en_A1A2_2022.pdf (accessed on 12 April 2023)
5. Laboratory biosafety manual, WHO
https://www.who.int/publications/i/item/9789240011311 (accessed on 12 April 2023)
6. Directive 2000/54/EC of the European Parliament and of the Council of 18 September 2000 on the protection of workers from risks related to exposure to biological agents at work (seventh individual directive within the meaning of Article 16(1) of Directive 89/391/EEC)
https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1375443992555&uri=CELEX:32000L0054 (accessed on 12 April 2023)

3. Regulations for supply of material and transport security:

1. European Agreement concerning the international carriage of dangerous goods by road (ADR) regulations
https://www.un-ilibrary.org/content/periodicals/24118613 (accessed on 12 April 2023)
2. IATA regulations
https://www.iata.org/en/programs/cargo/dgr/ (accessed on 12 April 2023)
3. International postal union requirements
https://www.upu.int/en/Universal-Postal-Union/About-UPU/Acts (accessed on 12 April 2023)

4. Regulation (EU) 2021/821 governing the EU's export control regime for dual-use microorganisms
https://eur-lex.europa.eu/eli/reg/2021/821/oj (accessed on 12 April 2023)
5. Commission implementing regulation (EU) 2019/2072 as regards protective measures against pests of plants
https://eur-lex.europa.eu/eli/reg_impl/2019/2072/oj (accessed on 12 April 2023)

MIRRI IS21

IMPLEMENTATION AND SUSTAINABILITY FOR THE 21ST CENTURY

MICROBIAL RESOURCE RESEARCH INFRASTRUCTURE