# OECD BEST PRACTICE GUIDELINES ON BIOSECURITY FOR BRCS


ORGANISATION FOR ECONOMIC CO-OPERATION
AND DEVELOPMENT

# ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 30 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

***TABLE OF CONTENTS***

## PREFACE

This document contains the Best Practice Guidelines for Biosecurity for Biological Resource Centres (BRCs). The Guidelines were endorsed by OECD member[1] countries in March 2007. The Member countries further endorsed a number of recommendations pertinent to these guidelines including:

*i)* The member countries of the OECD take steps to encourage the dissemination of these best practice guidelines and implementation of best practices amongst the potential user community;

*ii)* The user community itself (including, but not only, through the World Federation of Culture Collections) should not wait for government action but should immediately consider how to move towards implementation of the best practices set out here;

*iv)* Implementation of the best practices, including the impact of such implementation, should be reviewed periodically;

*v)* The best practice guidelines set out here represent the current state of the art for best practice, but should be monitored and kept under periodic review so that they can be updated to take account of scientific, technological and management advances.

The full set of recommendations, as well as background material and complementary guidelines, can be found in *OECD Best Practice Guidelines for Biological Resource Centres, OECD, 2007.*

1. The Guidelines were endorsed by the OECD Working Party on Biotechnology at its 21st Session on 19-21 February 2007 and they were subsequently endorsed by the OECD's Committee on Scientific and Technological Policy (CSTP) at its 89th CSTP meeting in March 2007.

## BACKGROUND

Biological resources – living organisms, cells, genes, and the related information – are the essential raw materials for the advancement of biotechnology, human health, and research and development in the life sciences. Such biological resources are the source materials for scientific investigation and R&D that lead to discoveries that will support the progress of biotechnology and the bio-industries. Ensuring the proper maintenance and supply of biological resources is thus essential for the future advancement of biotechnology and its contribution to the growth of the bio-economy.

In order to meet modern demands for advancements of biotechnology and life sciences, the OECD in 2001 introduced a new concept of repositories and providers of high quality biological materials and information: the Biological Resource Centre.

Biological resource centres are[2]:

> *"an essential part of the infrastructure underpinning biotechnology. They consist of service providers and repositories of the living cells, genomes of organisms, and information relating to heredity and the functions of biological systems. BRCs contain collections of culturable organisms (e.g. micro-organisms, plant, animal and human cells), replicable parts of these (e.g. genomes, plasmids, viruses, cDNAs), viable but not yet culturable organisms cells and tissues, as well as data bases containing molecular, physiological and structural information relevant to these collections and related bioinformatics. BRC must meet the high standards of quality and expertise demanded by the international community of scientists and industry for the delivery of biological information and materials. They must provide access to biological resources on which R&D in the life sciences and the advancement of biotechnology depends".*

Many BRCs are entrusted with the maintenance and exchange of hazardous biological resources. Society confers trust in BRCs as custodians of such materials, demanding that responsibility is taken for their safe use. In this context, culture collections have long recognised the duties of implementing proper containment procedures for hazardous biological material to safeguard workers against accidental exposure and acting in accordance with legislation on export controls and transport safety measures. More recently, the menace of bio-terrorism has changed the geo-political landscape, and consequently facilities that handle materials and information that could potentially be of "dual-use" have the added responsibility to make special efforts to secure against loss or theft.

The prospect of bioterrorism gives rise to the need to protect facilities that work with, store or transfer dangerous biological material from being intentionally misused for malevolent ends. Thus, to contribute most effectively to scientific and economic development, BRCs should not only promote scientific openness but also a sense of security.

---

2. "Biological Resource Centres: Underpinning the Future of Life Sciences and Biotechnology", ISBN 92-64-18690-5, 2001, OECD, Paris.

The *Best Practice Guidelines on Biosecurity for BRCs* are provided to support governments in the recognition of BRCs, and describe the methods and protocols for secure maintenance and provision of biological materials. They are designed to secure all types of biological materials (*e.g.* plant-, animal-, micro-organism- and human-derived) in proportion to the risk they present, and thereby marginalize any obstacles that BRCs might face in carrying out their function to provide quality assurance and rapid supply of biological materials for research, public health and economic development. Tailoring the level of security measures to the actual needs of diverse BRCs implies the utilisation of a mechanism capable of identifying which biological materials need to be secured. To address this fundamental point, some countries have adopted a list-based approach to biosecurity, whereby a list is established of biological materials that are deemed in need of special security measures and there is a clear and absolute distinction between those organisms that are on the list – and require specified additional security measures – and those that are not, and hence require no additional security above and beyond what is normally in place at facilities.

Given the risk of mistakenly excluding a hazardous biological material from such a list, the *Best Practice Guidelines on Biosecurity for BRCs* adopt an approach consisting of two key components: performing a risk assessment of the various biological materials held in collections and recommended risk management practices to reduce the risk of their loss or theft. The first key component assigns materials to one of four biosecurity risk levels: high, moderate, low or negligible, according to the degree of risk the biological material presents. The second key component contains measures tailored to the level of biosecurity risk that a biological material presents. Applying a graded approach is intended to better target the resources allocated to security by BRCs and to avoid establishing excessive security measures.

These best practice guidelines are intended to apply to all BRCs, irrespective of the type of material they hold and supply. However, given that the principal target is the biosecurity of pathogens, the best practice guidelines will in particular apply to micro-organism domain BRCs.

## OECD BEST PRACTICE GUIDELINES ON BIOSECURITY FOR BRCS

### Introduction

Biological resources underpin all biological sciences research. They provide the source material for scientific investigation, leading to many of the discoveries on which biotechnology is founded. Providing for high quality maintenance and rapid low-cost exchange of biological resources and quality information on them is a key issue for efficient advancement of the biological sciences. Quality assurance and protocols followed by Biological Resource Centres (BRCs) meet this need.

BRCs espouse openness of information and the ability to exchange material quickly; they therefore need to provide certain safeguards that such material and information will not be misused for nefarious purposes. The prospect of bioterrorism generates the need to secure facilities that work with, store or transfer dangerous biological material to ensure that such materials are not susceptible to misuse for malevolent ends. Thus, to contribute most effectively to scientific and economic development, BRCs should not only promote scientific openness but also a sense of security. The two goals are equally important and should be balanced and should be mutually reinforcing.

To deliver such a balanced and mutually reinforcing effect the aim of biosecurity best practice guidelines for BRCs is to reduce the probability that dangerous biological material could be obtained by unauthorised persons and deployed to cause harm, without unduly hindering research or being financially burdensome. Such best practice guidelines should be clearly articulated and grounded in an understanding of the biological material and the operations of BRCs.

### 1. General Provisions

The biosecurity best practice guidelines stated herein provide a basis for establishing best practices to secure the maintenance and provision of biological materials held by BRCs. They are designed to be implemented in conjunction with the general operational guidelines[3] for all BRCs and the applicable specific domain best practices for BRCs.

BRCs should implement these biosecurity best practice guidelines in a manner that does not conflict with obligations under national, local and/or international laws and regulations.

### 2. Scope

These biosecurity best practice guidelines are designed to apply to BRCs. They propose a framework for risk assessment of materials held within a BRC as well as a framework that sets out best practices for management of such risk.

The frameworks for risk assessment and risk management contained herein provide tangible tools for biosecurity. These are necessary but not sufficient to ensure biosecurity, however. Just as important will be a demonstrable culture of responsibility and awareness of security throughout a BRC. The assignment of an individual within a BRC who has, as part of his/her responsibilities, the general oversight of procedures within a BRC to ensure biosecurity is essential to achieve best practice and will contribute towards the said culture of security. The management and staff of a BRC should also

3. OECD Best Practice Guidelines for Biological Resource Centres, OECD, 2007.

share a sense of responsibility for biosecurity and a BRC should be able to demonstrate that this is the case.

## 3. Definitions

The definitions in *General Best Practice Guidelines for all BRCS*[4] apply with the additions below.

- "Biosecurity": Institutional and personal security measures and procedures designed to prevent the loss, theft, misuse, diversion or intentional release of pathogens, or parts of them, and toxin-producing organisms, as well as such toxins that are held, transferred and/or supplied by BRCs**.**
- "Risk assessment": The process of identifying sources of potential harm associated with the loss, theft, misuse, diversion or intentional release of pathogens, or parts of them, and toxin-producing organisms, as well as such toxins that are held, transferred and/or supplied by BRCs, assessing the likelihood that such harm will occur and the consequences if that harm occurs
- "Risk management": The process of weighing policy alternatives, considering risk assessment and other factors relevant for biosecurity, and selecting appropriate prevention and control actions**.**
- "Security breach": A security breach is any violation of the biosecurity best practice guidelines where these are intended to be in place as best practices.
- "Risk communication": The interactive exchange of information and opinions among personnel of the BRC and, where appropriate, other parties, concerning risk-related factors and risk perceptions.

## 4. Assessing biosecurity risks of biological material

BRCs should ensure that a detailed inventory of the different biological materials they hold is available.

BRCs should conduct a risk assessment of the biological materials in their inventories for the purpose of assigning such materials to biosecurity risk levels, which may be assigned as high, moderate, low or negligible (see Table 1). The level of biosecurity risk of biological material should be determined according to the best available information on its potential for malicious misuse (including economic consequences) as well as its virulence**.** Risk assessment should address the potential of biological materials, should they be obtained and misused by unauthorised persons, to cause harm to the health of humans, crops, livestock or infrastructure.

The provision of biosecurity should be regarded as a benefit to society at large. The burden of risk analysis should thus be shared collectively by BRCs and the broader science policy community. BRCs should engage in and together develop expert networks that can contribute to the provision of risk analysis.

BRCs should share their experience with other BRCs as regards the results of qualitative risk assessment and the reasons for assigning the biosecurity risk level of a particular biological material, and make all such documentation available to competent national authorities.

4. General Best Practice Guidelines for all BRCs are set out in the "*OECD Best Practice Guidelines for Biological Resource Centres, OECD, 2007*".

BRCs should determine a biological material's biosecurity risk level as a function of its potential for malicious misuse and its virulence. Establishing the biosecurity risk level of a particular material is instrumental to applying the Biosecurity Risk Management Practices in Section 6 below.

BRCs should assess potential for malicious misuse based on the following key factors:

- Availability: the number of facilities that stock the biological material and their geographical distribution.
- Amplification: the ease with which the biological material can be replicated, for example whether it can be grown in culture and its growth rate.
- Skills and knowledge: the ubiquity or rarity of the skills and knowledge necessary to amplify and/or genetically modify the biological material.
- Dispersal: the ease and effectiveness with which the biological material can be dispersed, such as by air, water, food or by other means into the environment. This might include (but not be limited to) a biological material's aerosolisation and inhalation characteristics.
- Environmental viability: the hardiness of the biological material across a range of temperatures, humidity levels, light exposures.
- Countermeasures: the existence of and ease of access to prophylaxis, post-exposure treatments and detection and decontamination measures.
- Economic consequence: the extent to which the biological material may be used to bring about harmful economic consequences for humans, crops, livestock or infrastructure.

BRCs should assess virulence based on the following key factors:

- Infective dose: the smallest quantity of the biological material necessary to cause infection.
- Pathogenicity: the disease-causing ability of the biological material.
- Lethality: the ability of the biological material to cause death to the host.
- Transmissibility: the ease with which the biological material can spread either by vector to host, or host to host.

In addition to the key risk factors set out above, other factors could materially affect the assessment of a biological material's potential for malicious misuse as well as its virulence. Where such factors are known it is the responsibility of the BRC to ensure that due account is taken of them in determining the overall biosecurity risk level of a biological material.

It is important to remember that in some cases, one risk factor may be so significant that it may determine the overall risk rating for a particular biological material. Thus, BRCs should carry out risk assessment in such a manner that risk factors are weighed.

In conducting risk assessment, if there is doubt as to whether a particular factor of a biological material should be characterised as high, moderate, low or negligible, BRCs should consider assigning that factor to the higher of the two possible levels. This need not imply that the overall biosecurity risk level for biological material is deemed higher.

BRCs, with the broader scientific community, should take steps, as a priority, to develop common methodologies for risk assessment and should seek to develop quantitative and qualitative tools and assessments that assist in completing appropriate and comparable risk assessment. For example, they

may conduct statistical analysis for the purpose of establishing average biosecurity risk levels for the same type of biological materials, and to signal conflicting biosecurity risk levels, in different BRCs. Reporting will also allow the establishment of a data base that BRCs may use as a reference. Such an approach will permit the harmonisation of data generation, and thus lead to an increasingly harmonized framework of risk assessment and risk management amongst BRCs. In developing common tools and methodologies, BRCs, with the broader scientific community, should be sure to draw on appropriate existing – including international – tools and methodologies. For example some list-based approaches currently used to assign risk may be deemed as useful inputs to risk assessment for the purpose of biosecurity.

## 5. New acquisitions/re-assessment of inventory

BRCs should make biosecurity risk assessment, as described in Section 4, part of the acquisition process of new biological material.

When being transferred between BRCs, a summary of a biological material's risk assessment should be made available to the recipient BRC. A new risk assessment should only be conducted if, after reviewing the summary, there appears to be new circumstances or information that affects the original assessment; in such case, the procedure for risk assessment set-out in Section 4 should be followed.

BRCs should re-assess the biosecurity risk level of materials for which there is new information about their virulence or potential for malicious misuse.

## 6. Biosecurity risk management practices

BRCs should implement the biosecurity management practices contained in sections 6.1-6.9 below in a graded manner to reflect the level of biosecurity risk of biological materials.

Risk management applies to biological material at all times, including the receipt, storage, use, transfer and disposal of materials.

BRCs should establish a timetable for internal audits to check for the level of compliance with the risk management practices. These evaluations should conform to the rolling audit and review programme as described in the document *General Best Practice Guidelines for all BRCs* Section 13.3.

BRCs should designate a biosecurity officer, at operational level within the BRC, whose responsibility it is to ensure internal compliance with the Biosecurity Best Practice Guidelines.

### *6.1. Physical security of BRCs*

BRCs should conduct all activities with biological material in an area that corresponds to the appropriate biosecurity risk level resulting from the application of the biosecurity risk assessment described in Section 4. A potential scheme of physical security levels is given in Table 1 below.

**Table 1. Potential scheme of physical security applicable to biosecurity risk levels associated with the BRCs**

| Biosecurity risk level | Physical security |
|---|---|
| Negligible or Low | General security area |
| Moderate | Restricted area |
| High | High security area |

BRCs should design (or adapt the design of existing construction of) their physical facility to reflect the requirements of sections 6.1.1-6.1.3 below. BRCs should supplement the general security area (6.1.1) by additional layers of physical security within the facility, if they possess biological material that presents a high or moderate biosecurity risk level. Biological material presenting a moderate biosecurity risk should be stored and worked with primarily in a restricted area (6.1.2), whereas biological material presenting a high biosecurity risk should be stored and worked with in a high security area (6.1.3).

*6.1.1 General security area*

BRCs should implement physical security measures that provide a general security barrier against theft and persons gaining unauthorised access to facilities and the material therein. The area enclosed by the general security barrier typically marks the physical boundary of the BRC. The general security barrier should be equipped with access controls, typically available to all staff at the facility. Access controls can be in the form of manual keys, electronic key-cards, presentation of staff ID badge to security guard etc. The general security area may or may not be equipped with a 24-hour intrusion detection system.

*6.1.2 Restricted area*

The restricted area is characterised by an additional layer of security and access controls through which only those staff authorised to have access to the materials held within may pass. Access to a restricted area requires an additional access item that is only available to individuals who are authorised to access the materials held within. The access item may be a manual key, key-card, electronic access code or a specific ID badge signalling that the individual has a different level of access than staff with access to the general security area only. Restricted areas should be enclosed on all sides within the general security area, *i.e.* the restricted area should not share a boundary with a public area. The restricted area should be equipped with a 24-hour intrusion detection system.

*6.1.3 High security area*

The high security area should be nested within a restricted area and should not under any circumstances share a physical boundary with the general security area. The high security area is characterised by an additional layer of security and access controls through which only those staff authorised to have access to the materials held within may pass. Access to the high security area requires an additional access item that is only available to individuals who are authorised to access the materials held within. The access item, key, key-card, electronic access code, specific ID badge should signal that the individual has a different level of access than staff with access to only the general or general and restricted areas. The high security area should be equipped with a 24-hour intrusion detection system.

The construction of restricted and high security areas should be such that any apertures (windows, ventilation shafts) that are sufficiently large for a person to gain entry through are secured to prevent this. Emergency exit doors should be releasable only from the inside, unless prevailing safety codes provide otherwise.

BRCs should maintain equipment/facility maintenance logs of the security areas, including names and affiliation of maintenance personnel.

### *6.2. Security management of personnel*

The BRC manager should ensure that attentive management practices in the supervision of staff are the norm.

BRCs should institute security screening, in line with national privacy law, and set in place best practice guidelines describing how decisions on appointments (or granting existing staff a higher access level) should be taken according to the nature of the facts that emerge about the individual. Background checks of staff whose duties require them to have access to material that presents a high or moderate biosecurity risk should be conducted prior to the granting of access to such biological materials.

All staff should be issued with an identification token, preferably equipped with a photograph of its issued holder, and providing information as to their level of access. Identification tokens should be worn at all times except in circumstances where doing so would present a health and safety risk (when wearing a biohazard suit for example). Identification tokens should be surrendered upon termination of employment at the BRC. BRCs should keep records of current and former employees, while paying due respect to their privacy.

### *6.3. Security management of visitors*

BRCs should establish a system of security controls for visitors.

A BRC's system of security controls should include a list of the types of visitors that it allows to enter its facility and classifies whether the visitor should be escorted or unescorted.

Unescorted visitors should be subject to the same security management procedures as BRC personnel (see section 6.2). Alternatively the facility may choose to accept the security clearance conferred on the visitor by a government agency, or other appropriate body, provided that security clearance is current.

In general, escorted visitors should not have access to restricted or high security areas.

BRCs should maintain visitor logs, ensure that visitors do not enter the facility with prohibited items, and issue visitors with a colour coded badge (or equivalent means) according to the level of biosecurity risk to which they have access. Badges should either automatically expire when the visitor leaves, or be taken from the visitor on exiting. Appropriate visitor-to-escort ratios should be established for different security areas (for tours within the general security area 10:1 or higher may be appropriate, whereas escorting maintenance staff within the high security area may require a 1:1 ratio).

Permission to visit the facility should be granted by the manager of the BRC or a designee. Decisions on visits to restricted and high security areas should be taken in consultation with the biosecurity officer (where such an individual is distinct from the manager of the BRC). Only those personnel that have the appropriate level of access should escort visitors within restricted and high security areas.

### *6.4. Incident response plan*

BRCs should devise and adopt an incident response plan, which sets forth a protocol to be followed by BRC staff for recording, reporting and investigating security breaches. Guided by applicable laws, BRCs should determine how to report investigations of security breaches.

BRCs should ensure that every staff member (including non-technical staff) is fully notified of the incident response plan and trained in the actions they should take in the event of a security breach.

The incident response plan should indicate the reporting requirements in case of a security breach. BRCs should alert the responsible national authorities if a security breach involves biological material with a high or moderate biosecurity risk level, and be prepared to communicate information on associated risks to the local community if so requested by competent national authorities.

For security breaches involving biological material with a high or moderate biosecurity risk level, the incident response plan should identify the internal staff and external national authorities to whom the security breach is to be reported, in what order, and any other actions they need to take. These actions should include immediately instigating appropriate biosafety measures to reduce any health and safety risks to laboratory staff and the local community arising from the breach, and in as far as it is safe to do so, avoid disturbing the scene of the breach and any evidence until authorities arrive.

The incident response plan should identify individuals responsible for retrieving and compiling information that may assist investigating authorities, including where relevant, a list of people who have legitimate access to the material, the biosecurity risk level assigned to the biological material or data compromised (*e.g.* infective dose, pathogenicity, lethality, transmissibility, environmental viability, availability of therapeutic agents) and the inventory of requests received for the material.

### *6.5. Staff training and developing a biosecurity-conscious culture*

BRCs should devise and implement a biosecurity training course to instruct relevant staff (both technical and non-technical staff) in the biosecurity procedures of the facility. The training course should explain to staff the key elements of the Risk Management Practices and ensure that staff are aware of their responsibilities and the procedures that should be followed during the course of their work. The course should give staff specific instruction on what constitutes a breach of security procedures and if appropriate, provide information about disciplinary sanctions that will be applied if a staff member deviates from the BRC's biosecurity policy.

In particular, the course should instruct on the Incident Response Plan, ensuring that all staff are fully aware of the actions they should take if they detect a security breach, or witness activity that they deem suspicious on security grounds.

The biosecurity training course should comprise one element of the general orientation course that new staff typically undergo.

Appropriate risk communication and the creation of a biosecurity-conscious culture in the community are important elements in establishing biosecurity. In addition to undertaking sufficient biosecurity measures, a BRC should conduct its activities in a transparent manner and strive to build trust in its relations with the local community

### *6.6. Material control and accountability*

BRCs should establish a system of material control and accountability, which includes conducting and maintaining inventories of biological materials in their collections and identifies individuals who have access to or custody of biological materials at any point in time.

The system should provide accurate knowledge of what biological materials exist in a BRC, where those materials are, and who has access to them or custody of them at any given time. Material control and accountability applies to all biological materials held by BRCs, including those with only negligible or low biosecurity risk associated with them. Individual vials need not be counted except in the case of high biosecurity risk level materials.

### *6.7. Supply of material*

BRCs may grant requests from facilities that seek to acquire, use and maintain biological material that presents a negligible or low risk, subject to national legislation.

Biological material that presents a moderate or high biosecurity risk should only be transferred to facilities that ensure biosafety and biosecurity measures appropriate to handle such material are in place.

BRCs should document all acquisition requests in particular for high and moderate biosecurity risk level materials, including requests refused and the reason for refusal. BRCs should be able to provide competent national authorities with a record of all acquisition requests for such materials whether the request was accepted or declined, if requested by such national authorities.

In order to bring to light in a timely manner that biological materials have been lost or diverted during transport, BRCs should condition dispatch of biological material with a high or moderate biosecurity risk level upon agreement of the receiving party to provide notice of successful receipt in their as agreed timeframe.

### *6.8. Transport security*

BRCs should institute procedures that secure material during packaging and transport to reduce the risk of theft.

Internal and external transfers of biological material that present a negligible or low biosecurity risk do not require any additional security measures other than those required by national or regional/international regulations.

#### *6.8.1 Internal transport*

Biological material that poses a high biosecurity risk should neither be left unattended nor temporarily stored outside the high security area.

BRCs should employ a strict chain of custody approach to the internal transfer of biological material that presents a moderate or high biosecurity risk and movement from one high security or restricted area, via a restricted or general security area, to another high security or restricted area.

This procedure should aim to be as minimally burdensome as possible while allowing subsequent analysis of such transactions and transfers made within the scope of the preceding paragraph.

#### *6.8.2 External transport*

BRCs should follow the WHO Guidelines on International Regulations for the Packaging and Transport of Infectious Substances to ensure safe and secure packaging and transportation of biological material.

Biological material exempt from the WHO guidelines (non-infectious micro-organisms allocated to Risk Group1) may be sent by (air) mail or other means of transport according to the Universal Postal Union (UPU) requirements.

BRCs should follow the International Air Transport Association (IATA) Dangerous Goods Regulations (DGR) and other applicable regulations, including those for road transport, to ensure that all requirements for packaging and shipping dangerous goods on ground and air are met.

BRCs should ensure that staff responsible for the distribution of biological material have the necessary knowledge and training to comply with applicable national and regional/international laws and regulations. Staff responsible for the distribution of dangerous goods (including infectious substances) via air should have the shipper's training certificate as required by IATA.

### *6.9. Security of information*

BRCs should undertake an information risk assessment, to determine what information presents a biosecurity risk and take steps to protect information that could reasonably be used to facilitate the theft of high or moderate biosecurity risk material (*e.g.* access codes).

#### *6.9.1 Information that relates to access to materials*

Information that could reasonably be used to facilitate the loss or theft of biological materials with a high or moderate biosecurity risk level should be protected by proportionate measures to ensure the security of this information. The information should be secured against unauthorised access by appropriate physical and/or electronic means (depending on the format in which the information is stored and the resources available to the BRC).

Access to information pertaining to biological materials associated with high or moderate biosecurity risk levels should be granted on a need-to-know basis, and granted only to those individuals with security clearance to access material at the same biosecurity level as the information sought. For example, individuals with clearance to access moderate biosecurity level material should be able to access (if necessary) information up to that security level, but not above.

#### *6.9.2 Information that relates to the collection*

BRCs should develop a policy to guide them in deciding what kinds of information relating to the collection should purposefully be withheld from entering the public domain.

The BRC staff should be aware that their repository of knowledge could present a security risk. BRCs may choose to address this issue through encouraging staff to adopt a code of conduct specific to biosecurity.

## NOTES

These notes are to be read jointly with their corresponding sections found in the biosecurity best practice guidelines.

**Scope**

BRCs distinguish between biosecurity and biosafety measures. Biosafety entails the use of containment principles, technologies and practices that are implemented to prevent unintentional exposure to pathogens and toxins, or their accidental release. Biosecurity is intended to deter or detect the loss or theft of dangerous biological materials for illicit or malicious purposes. These biosecurity best practice guidelines focus on preventing unauthorised access to dangerous biological materials in BRCs. They are not intended to address biosecurity in other types of facilities, nor do they address specific measures related to crisis management in the event of a security breach.

**Biosecurity risk management practices for BRCs**

The biosecurity officer need not be a separate, full-time position; its functions may belong to the responsibilities of the BRC manager or another employee of the BRC.

***6.1. Physical security of BRCs***

The purpose of physical security measures is to minimize opportunities for unauthorized entry into BRCs, and to prevent the unauthorized removal of materials from their facility. Physical security measures can be manual, such as locks on internal and external doors, freezers and storage cabinets, or electronic, such as electronic access and biometric access controls, or they can be based on manpower (private security guards). Intrusion detection sensors and cameras, although not physical barriers, can provide an instant alert in the case of a security breach. In exceptional circumstances biometric controls may be deemed appropriate.

***6.3. Security management of visitors***

BRCs possessing high or moderate biosecurity risk material should develop a policy addressing prohibited items for both staff and visitors and inform staff about what particular items are prohibited.

Although escorted visitors generally should not have access to restricted or high security areas, some circumstances (such as essential maintenance work) may require it.

***6.4. Incident response plan***

The severity of a security breach should be evaluated in accordance with risks that arise as a consequence of it. For example, a missing link in the documented chain of custody should be considered a less severe security breach than unauthorized entry into the facility or misappropriation of biological material.

***6.5. Staff training and developing a biosecurity-conscious culture***

BRCs should seek to raise awareness of the need to secure biological materials against their unauthorised acquisition and misuse by holding seminars, information campaigns and other activities as they consider appropriate to the nature of the facility and the tasks performed by their staff. An

important component of developing a biosecurity-conscious culture is the development of a code of conduct by staff.

### *6.7. Supply of material*

It is incumbent on the requesting facility, not the BRC, to prove to the BRCs satisfaction that it has put in place biosafety and biosecurity measures appropriate to handle high and moderate biosecurity risk level materials.

*6.8.2 External security*

The WHO Guidelines may be found at the following web link:
http://whqlibdoc.who.int/hq/1997/WHO_EMC_97.3.pdf.

The International Postal Union requirements may be found at the following web link:
http://ibis.ib.upu.org.

The IATA regulations can be found at the following web link: http://www.IATA.org/cargo/dg.

An example of transport regulations is the European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR regulations). The ADR regulations can be found at the following web link: http://www.unece.org/trans/danger/publi/adr/ADRagree_e.pdf.

*6.9.1 Information that relates to access to materials*

This includes information pertaining to the facility (physical plans detailing the layout of the facility and the location of the master control of electrical and communication services that are essential for keeping security barriers in place), personal information on employees that could be used for blackmail, sensitive documentation such as a review that points to weaknesses in a facility's security programme, and information that could potentially assist in gaining unauthorised access to biological materials and inventories.

The key question in conducting the information risk assessment is whether possessing the information would permit the holder to severely compromise the health of humans, crops, livestock or infrastructure.

*6.9.2 Information that relates to the collection*

Information that relates to the collection includes detailed information on organisms, such as that relating to environmental hardiness, aerosolisation, cultivation method, sequence data *etc.* Such information, in particular that relating to organisms that present a high or moderate biosecurity risk, can present a security risk itself.

In deciding what information relates to the collection, BRCs may be guided by the Journal Editors' Statement on Scientific Publication, see: *Security Journal Editors and Authors Group, Proceedings of the National Academy of Sciences* (PNAS), February 18, 2003, Vol. 110, No. 4, pp. 1464.

A source for various laboratory biosecurity codes of conduct can be found at the following web link: http://www.biosecuritycodes.org/.