Biosecurity Policy DRAFT

Introduction and Purpose

There are a number of new rules and regulations that govern the use of certain biological agents and toxins. In particular, Section 2.6 of the Health Canada Laboratory Biosafety Guidelines requires that all research laboratories have a biosecurity plan in place. Biosecurity measures are implemented to prevent the theft, misuse or intentional release of pathogens.

In general, none of the pathogens used at the iCAPTURE Centre are above containment level 2. These pathogens include the following: adenovirus, parainfluenza virus, rhinovirus, respiratory syncytial virus, and coxsackie virus. However, the Centre is located at St. Paul's Hospital (SPH), in a downtown Vancouver area, and there is a higher risk of potential security breaks.

The iCAPTURE Centre must assess the risk of an agent and determine the physical, personnel and pathogen controls required. The Centre must have a plan to address a biosecurity incident and emergency response. Research groups must have a lawful purpose to possess, use and transport the agents and procedures to identify and characterize the agents held at any facility/laboratory.
The Biosecurity Policy specifies security requirements for laboratories using special agents. The iCAPTURE Centre requires that all users of biological agents adopt the requirements outlined in this policy.

The iCAPTURE Centre currently has a Biosecurity Committee that will meet every 6 months to monitor compliance with the policy as well as to review and update it.

1. Physical Protection

All the laboratories at the iCAPTURE Centre are behind an electronic locking system. The self-closing doors are kept locked at all times, accessible only to personnel who have attended the safety orientation for the laboratory and who have been issued access/photo ID cards or keys. SPH Security also keeps an electronic log for access cards. For extra security precautions, a video camera is operating across from the elevator on the 2nd floor McDonald wing.

iCAPTURE personnel using human pathogens or toxins must report immediately to their supervisor, the McDonald Operations Managers (MOM), SPH Security, and UBC Biosafety Office if any of the following events occur:

- Loss or compromise of their access cards, keys, passwords
- Suspicious persons or activities
- Loss or theft of human pathogens or toxins
- Release of select agents or toxins
- Sign that inventory, material transfer agreements (MTA), and use records of select agents or toxins have been altered or otherwise compromised.

Data, IT, and Cyber Security

- The greatest risk to information security is inadvertent disclosure by employees. The following measures will be taken to minimize these risks.

- Hiring Permanent Employees: Supervisors are to review applications, carry out interviews and check references before making their final selection.
- Work-Study Students and Temporary Employees: Confidentiality and safeguarding of information should be covered by each work-study employer as students are hired to work in each department. Work-Study and other temporary employees shall have unique email addresses instead of sharing an address with past, present, or future temporary employees.
- Existing Employees: All current employees who have access to human pathogens and toxins information must be informed of information security requirements.
- Ongoing Training: As part of the annual review process, the supervisor will review information security requirements with their respective employees or any employee who has access to human pathogens and toxins select agent information.
- Access to Human Pathogens and Toxins Information: Only employees whose job duties require them to access select agent information shall have access.

Information Systems

Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Lack of adequate procedures and technical controls creates a risk of unauthorized access to the information systems, and of accidental loss in the event of disasters or system failures. The following measures will be taken to minimize this risk.

- Paper Storage Systems: Supervisors should instruct employees on the need to keep confidential files out of public view, and also provide for storage of confidential files in locked cabinets wherever feasible. Paper shredders are available, as well as locked confidential paper recycling bins.
- Computer Information Systems: The Centre and the University have data ownership and access procedures that apply to all centrally managed data supported by administrative information systems.
- iCAPTURE Centre Policy Concerning Acceptable Use of IT Resources: All Employees and students will receive, read and understand and sign a form regarding the iCAPTURE Centre Policy on Acceptable Use of Computer Systems Manual and the iCAPTURE Centre Policy on Computer Passwords.
- iCAPTURE Centre Privacy Policy: All Employees and students will sign the Confidentiality Agreement form.

2. Personnel Suitability/Reliability

Every new employee will be informed about the Biosecurity plan during the new employee orientations. The training will provide information about restricted access areas, how they are identified and what unauthorized personnel must do to access these areas.

Personnel working with biosecurity agents of concern have to be qualified and properly trained by direct supervisors.

Personnel access may be restricted to areas where biosecurity agents of concern are used, stored or otherwise present. All personnel entering into a restricted area will need to log in/out. Visitors will be escorted to the restricted area by an authorized employee and be required to log in/out. Authorized

personnel will not share their means of accessing the area where select agents or toxins are stored and used. This includes passwords, keys, keycards, or combinations.

3. Pathogen Accountability

Pathogen and toxins users must keep a record of the agents location, how it is used, inventory, transfers (external/internal), destruction and access.
Copies of logs will be provided to the University Biosafety Office during inspections. Researchers will keep record of logs indefinitely. The following logs are required:

- Name, characteristic and source date of agent
- The quantity acquired, the source and date of acquisition
- Quantity held on the date of the first inventory (toxin only)
- Current quantity held (toxin only)
- The quantity used and dates of the use (toxin only)
- The name of each person who has accessed any select agent or toxin
    - The select agent or toxin used
    - Date removed
    - The amount of toxin used
    - The date agent was returned to storage
    - Quantity of toxin returned
- The quantity transferred within and outside the Centre, transfer date, recipient's name
- Shipping must conform to applicable TDG regulations. All shipments of biological agents will meet the packaging requirements defined by IATA "Shipping Infectious and Biological Substances."
- The quantity, volume or mass destroyed or otherwise disposed and the date of each action, including the decontamination method.

4. Biosecurity Incident and Emergency Response

Each laboratory with biosecurity agents of concern must have a plan to report and investigate security incidents. This plan includes:

- Unauthorized personnel in restricted areas
- Unauthorized removal of pathogens
- Breach of containment

Unauthorized personnel are not allowed in restricted areas. If members of the public are found in the restricted labs, SPH Security will be immediately notified.

Any security breach in a human pathogen/toxin use area must be immediately reported to the iCAPTURE MOM, iCAPTURE Director, SPH Security and UBC HSE Biosafety Office.

5. References

- *Laboratory Biosafety Guidelines*, 3rd Ed., Health Canada 2004, pp. 12-17.