CTRNet Standard Operating Procedure Physical Security at Facilities			
SOP Number:	04.001	Version:	e2.0
Supersedes:	4.1.001 e1.0	Category:	Facilities Management and Operations

Approved By:	CTRNet Management Group (CMG)	01-May-2012
	Per: Brent Schacter	31-May-2012
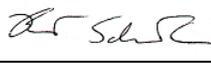
1.0 PURPOSE

Biobanks are intended to manage the safekeeping of Human Biological Materials (HBMs) in their custody. HBMs are a precious resource and each biobank should use basic security systems to provide a protective environment for the resource they control.

2.0 SCOPE

This standard operating procedure (SOP) outlines general elements and features that should be in place to provide a safe efficient and secure physical environment for the biobank.

3.0 REFERENCE TO OTHER CTRNET SOPS OR POLICIES

Note: When adopting this SOP for local use please reference CTRNet.

3.1 *CTRNet Policy: POL 2 Ethics*
3.2 *CTRNet Policy: POL 4 Privacy and Security*
3.3 *CTRNet Policy: POL 7 Material and Information Handling*

4.0 ROLES AND RESPONSIBILITIES

The policy applies to all personnel from CTRNet member biobanks that work at the biobank site or are the responsible custodians of the collection within the biobank.

Tumour Biobank Personnel	Responsibility/Role
All personnel	Maintaining Security at Biobank

5.0   MATERIALS, EQUIPMENT AND FORMS

Items listed in the following list are recommendations only and may be substituted by alternative/equivalent products more suitable for the site-specific task or procedure.

Materials and Equipment	Materials and Equipment (Site Specific)
Emergency Contact Lists	
Maintenance Documentation	

6.0   DEFINITIONS

See the CTRNet Program Glossary: http://www.ctrnet.ca/glossary

7.0   PROCEDURES

The facility should employ fundamental security systems to protect the collection. An efficient tumour biobank should be designed and have elements in place to provide a safe, secure and efficient work environment. Measures should also be taken to protect expensive and specialized equipment at the facility.

7.1   Facilities - General Procedures for Maintaining Security

7.1.1   Provide sufficient and secure space in the biobank for equipment being used and material being stored.

7.1.2   Provide basic security systems to ensure safekeeping of the collection. Monitor the systems adequately to allow for prompt response to any breach in security.

7.1.3   Designate a responsible individual (including designated back-up) to take necessary action in case of failure of systems.

7.1.4   Post the emergency contact information for responsible individuals and key personnel in a prominent location within the biobank.

7.1.5   Provide personnel with education and training about security and emergency procedures to ensure an appropriate response to any failure of systems that may occur.

7.2   Facilities – Temperature

7.2.1   Provide a suitable heating system to maintain ambient temperature to prevent freezing of water and drain lines.

7.2.2   When needed, provide suitable cooling to maintain adequate ambient temperature for electronic and mechanical equipment.

7.3   Facilities – Lighting

7.3.1   Provide adequate general and task lighting to ensure that the appropriate level of illumination is available to perform routine and specialized tasks undertaken at the biobank.

7.3.2   Provide back-up lighting for emergency situations.

7.4   Security Systems for Fire

7.4.1   Ensure that the fire prevention system is compliant with the codes and regulations in effect.

7.5 Facilities – Limiting Access

7.5.1 Define and create physical barriers around biobank resources to prevent physical intrusion.

7.5.2 Lock all doors and control entry to biobank facilities.

7.5.3 Where possible, limit access to biobank facilities to appropriate personnel and authorized staff.

7.5.4 Use physical, electronic and/or procedural controls to limit access to restricted and sensitive areas of the biobank.

7.5.5 Issue personnel with visible identification and controlled access keys. Upon termination of employment, make personnel surrender all identification and access keys.

7.5.6 Report lost or stolen access cards, deactivate these cards immediately and issue a new card as appropriate.

7.5.7 Review and keep up-to-date access rights, remove access for individuals that no longer need access.

7.5.8 Grant restricted access to authorized visitors or third party personnel.

7.6 Facilities – Back-up Power System

7.6.1 Ideally have an auxiliary power generation system in place to deal with loss of commercial power.

7.6.2 Keep a sufficient fuel supply for the emergency power generation system to ensure it will provide emergency power for at least 72 hours.

7.6.3 Ensure that important equipment, such as computers and freezers are plugged into the emergency power supply system – typically emergency plugs are identified by their color (red).

7.6.4 Avoid (if possible) opening of freezers and using sensitive equipment for the duration of the primary supply failure.

7.7 Facilities – Equipment Security

7.7.1 Protect equipment as needed to reduce risk of unauthorized access to data and HBMs stored in the biobank and to protect from loss and damage.

7.7.2 Maintain equipment correctly to ensure continued availability and integrity.

7.7.3 Allow only authorized maintenance personnel to carry out repairs and services to facilities equipment.

8.0 APPLICABLE REFERENCES, REGULATIONS AND GUIDELINES

8.1 Tri-Council Policy Statement 2; Ethical Conduct for Research Involving Humans; Medical Research Council of Canada; Natural Sciences and Engineering Council of Canada; Social Sciences and Humanities Research Council of Canada, December 2010.
http://www.pre.ethics.gc.ca/eng/policy-politique/initiatives/tcps2-eptc2/Default/

8.2 Best Practices for Repositories I. Collection, Storage and Retrieval of Human Biological Materials for Research. International Society for Biological and Environmental Repositories (ISBER).
http://www.isber.org/Search/search.asp?zoom_query=best+practices+for+repositories

8.3 US National Biospecimen Network Blueprint
http://biospecimens.cancer.gov/resources/publications/reports/nbn.asp

9.0 APPENDICES

None

10.0 REVISION HISTORY

SOP Number	Date revised	Author	Summary of Revisions
FS 002.001	2005	JdSh	Original
4.1.001 e1.0	2007	JdSh	Revised to make minor formatting changes and reviewed to reflect current practice at member banks
4.1.001	7/2011	GS	No revisions
4.1.001 e1.0	May 2012	CMG	• Grammatical and formatting throughout • Definitions removed • Revision History moved to bottom • Reference links updates • Updated SOP references • Title changed to Physical Security of Facilities • Section 2.0: deleted last sentence. • Section 7.1- Changed "security breach" to "failure of systems". • Deleted Section 7.3 - Facilities Air Flow • Revised Section 7.7-Back-up Power System • Changed section 7.6 to reflect the other SOPs that say to have back-up power for at least 72 hours.