CTRNet Standard Operating Procedure Database Backup Systems			
SOP Number:	3.1.002	Version	e1.0
Supersedes:		Effective Date	09 Jan 08
Subject:	Database Backup Systems	Category	Records Management and Documentation

Prepared By:		Aaron Suggitt & Jean de Sousa-Hitzler		
	Signature	Name	Title	ddMmmyy
Approved By:		Peter Geary	CEO	09 Jan 08
	Signature	Name	Title	ddMmmyy
Approved By:				
	Signature	Name	Title	ddMmmyy

REVISION HISTORY

SOP Number	Date Issued	Author (Initials)	Summary of Revisions
6.1.002	2008	JdSH	1st Release.

1.0 PURPOSE

Tumour banks or repositories are intended to manage the safekeeping of clinical data and other sample associated data in their custody. CTRNet has policies regarding security safeguards to protect data and personal information stored on its database against failure, loss and damage. Failure may occur due to user error (modifying or destroying the data on its own or through a user choice), media failure (failure of equipment such hard drive) or a catastrophic event such as a fire, flood, power outage, virus, or deliberate hacking. Back up systems must ensure that the information on the database can be completely and accurately recovered. CTRNet recommends banks strive to ensure data can be fully recovered on a daily basis. The aim is to limit data loss to no more than one day.

2.0 SCOPE

This standard operating procedure (SOP) outlines general elements and features that should be in place to ensure that information stored on its database can be recovered accurately, completely and in a timely manner.

3.0 REFERENCE TO OTHER POLICIES AND SOPS

1. CTRNet Policy: POL 004.001 Privacy and Security
2. CTRNet Policy: POL 007.001 Material and Information Handling Policy

4.0 RESPONSIBILITY

The policy applies to personnel from CTRNet member repositories who are responsible for the database system and the safekeeping of sample and participant related information.

Tumour Bank Personnel	**Responsibility/Role**	**Site Specific Personnel and Contact Information**
Information Technology (IT) Staff	Conducts backup/restores database according to specific bank plan.	
Bank Manager/Coordinator Bank Director	Participates in development of bank backup and recovery plan. Outlines recovery expectations.	
Tumour Bank management	Ensures adequate backup systems are in place	

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)**
Database back up system	
Removable backup media	
Offsite storage location	

6.0 DEFINITIONS

Backup: Procedures to routinely store and recover information held on the database.

Custodianship: Responsibility for safe keeping of tissue samples and associated data and control of their use and eventual disposal in accordance with the terms of the consent given by the participant and as regulated by the Research Ethics Board. Custodianship implies some rights to decide how the samples are used and by whom, and also responsibility for safeguarding the interests of donors.

Tumour Bank Application: Software and hardware system used to annotate, track and distribute biospecimens stored within the biorepository.

Safety: Processes, procedures and technologies to ensure freedom from danger or harm.

Database Management System (DBMS): A complex set of software programs that controls the organization, storage and retrieval of data in a database. Typical examples of DBMSs include Oracle, DB2, Microsoft Access, Microsoft SQL Server, Postgres, MySQL and FileMaker.

7.0 PROCEDURES

The facility must employ fundamental backup systems to protect the data stored on the database from damage and loss. In the case of user error, media failure or catastrophic events, the system should ideally be able to recover the information to the point before failure occurred. There should also be confidence that the information is complete and free of corruption.

7.1 Database Backup - General Description of Process

1. Each bank should develop a backup strategy based on:
    - Database size
    - Backup media available
    - DBMS used
    - Recovery requirements (Acceptable data loss)
    - Error detection (Undiscovered problems with data integrity that may require recovery for one or more older archive sets to locate and correct the problem.
2. Upon development of an acceptable backup plan, IT staff at the bank should implement and monitor regular backups.
3. Send regular backup copies to offsite storage in case of fire, flood, earthquake or other “Acts of God” which may destroy on-site archives.
4. Test data recovery at specific intervals as specified in the backup/recovery plan and record results. Test both individual records and full database recovery. Be sure to test offsite archival sets as well.

7.2 Database Backup – Routine Process

1. Routine steps will depend on the media used. Ideally, the backup system should be automated and not require daily user intervention (manual changing of backup tapes for instance) to reduce chance of error.
2. Perform validation to ensure the nightly backup completed successfully. Investigate any failed backups and resolve with the highest priority.

7.3 Database Backup – Frequency

1. Frequency is dependant on the recovery needs of the bank. As a guideline the database should be backed up nightly. In the event of catastrophic hardware failure, at most one day of data entry or changes may be lost.
2. Maintain a standard archive set to include 1 (one) year of archived data (CTRNet recommended).
    a. Keep a full monthly copy for a period of one year
    b. Use a set of 5 (five) weekly copies for each month
    c. Separate media for each day of operations (excluding off-days such as weekends and week-end copy)
3. Offsite Storage
    a. CTRNet recommends (at minimum) monthly copies be sent offsite, weekly is preferred.
    b. Where offsite storage is maintained, the service provider must be authorized by the host institution to handle sensitive data.

7.4 Database Backup – Recovery Plan

1. Base the bank recovery plan on acceptable data loss. The ability to recover data may also depend on the system hardware and DBMS used.

7.5 Database Backup – Audit and Validation of Recovered Data Security Systems for Fire

1. Develop a test plan to ensure backups are readable and store valid data.
2. Perform tests for full database recovery as well as individual record retrieval on a quarterly basis.

8.0 APPLICABLE REFREENCES, REGULATONS AND GUIDELINES

1. Tri-Council Policy Statement; 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, August 1998. http://www.pre.ethics.gc.ca/english/policystatement/policystatement.cfm
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
3. US National Biospecimen Network Blueprint http://www.ndoc.org/about_ndc/reports/NBN_comment.asp

9.0 APPENDICES

None