Procédure normalisée de fonctionnement Systèmes de sauvegarde des bases de données			
Catégorie:	Gestion et documentation des dossiers		
Numéro de PNF:	03.002	Version:	f2.0
Remplace:	3.1.002 f1.0	Date d'entrée en vigueur:	30 mai 2012

Approuvée par:	Comité administratif du RCBT (CAR)	01 mai 2012
	Par: Brent Schacter	30 mai 2012

1.0 INTENTION

Les banques de tumeurs doivent sauvegarder les données cliniques et les autres informations associées aux échantillons dont elles sont fiduciaires. La politique du RCBT à l'égard des sauvegardes de données vise à protéger les données et les informations personnelles entreposées dans ses bases de données contre les pannes, les pertes et les dommages. Une défaillance peut survenir en raison d'une erreur d'utilisation (modification ou destruction volontaire ou accidentelle des données), d'un bris d'équipement (panne du disque dur) ou d'un évènement catastrophique comme un incendie, une inondation, une panne de courant, un virus ou un piratage informatique. Les systèmes de sauvegarde doivent garantir que l'information contenue dans la base de données puisse être intégralement restaurée. Le RCBT recommande à ce que les biobanques s'efforcent de s'assurer que les données puissent être récupérées sur une base quotidienne. L'objectif consiste à limiter la perte éventuelle de données à une seule journée.

2.0 PORTÉE

Cette procédure normalisée de fonctionnement (PNF) trace les éléments généraux et les caractéristiques qui doivent être mis en place pour s'assurer que l'information entreposée dans une base de données puisse être intégralement récupérée et dans un laps de temps raisonnable.

3.0 RÉFÉRENCES À D'AUTRES PNFs OU POLITIQUES DU RCBT

Remarque: Lors de l'adoption de cette PNF pour un usage local, s'il vous plaît faire référence au RCBT.

3.1 *Politique du RCBT: POL 4 Vie privée et sécurité*
3.2 *Politique du RCBT: POL 7 Manipulation du matériel et de l'information*

4.0 RÔLES ET RESPONSABILITÉS

La PNF s'applique au personnel des banques membres du RCBT qui sont responsables du système de base de données, de la sauvegarde des échantillons et de l'information relative au participant.

Personnel de la banque de tumeurs	**Responsabilité/Rôle**
Personnel du département des technologies de l'information (TI)	Gère les sauvegardes et récupère les données en accord avec les règles définies par la biobanque.
Administrateur/coordonnateur de la banque, directeur	Participe au développement des besoins pour la sauvegarde et la récupération des données. Décrit les attentes de la récupération.

Administrateur de la banque de tumeurs	S'assure qu'un système de sauvegarde adéquat a été mis en place.

5.0 MATÉRIEL, ÉQUIPEMENT ET FORMULAIRES

Le matériel, l'équipement et les formulaires inscrits dans la liste suivante ne sont que recommandés et peuvent être substitués par des produits alternatifs/équivalents plus appropriés aux tâches ou aux procédures spécifiques aux sites.

Matériel et équipement	**Matériel et équipement (spécifiques au site)**
Système de sauvegarde de la base de données	
Support de sauvegarde amovible	
Lieu d'entreposage extérieur	

6.0 DÉFINITIONS

Voir le glossaire du RCBT : http://www.ctrnet.ca/glossary

7.0 PROCÉDURES

Les installations doivent comporter des systèmes de sauvegarde pour protéger les informations contenues dans la base de données des dommages et des pertes. Dans le cas d'erreurs d'utilisateurs, de bris d'équipements ou d'évènements nuisibles, le système devrait être capable de récupérer et restaurer intégralement l'information telle qu'elle était avant l'incident. Il devrait également fournir l'assurance que l'information est exempte de corruption.

7.1 Sauvegarde des bases de données – Description générale du processus

7.1.1 Chaque biobanque devrait développer une stratégie de sauvegarde basée sur :

- La taille des données entreposées
- Les supports de sauvegarde disponibles
- Le système de gestion de base de donnée (SGBD) utilisé
- Les exigences de récupération (Perte acceptable de données)
- L'erreur de détection - Problèmes d'intégrité des données qui requièrent la récupération d'archives plus ou moins vieilles afin de localiser la source de l'erreur et la corriger.

7.1.2 Se basant sur un plan de sauvegarde acceptable, le personnel IT de la banque devrait implanter et gérer des processus de sauvegardes réguliers.

7.1.3 Entreposer de manière régulière des copies des sauvegardes sur des sites extérieures afin de protéger les données d'évènements nuisibles pouvant détruire le site principal d'archivage (feu, inondations, tremblements de terre, catastrophes naturelles, etc).

7.1.4 Tester la récupération des données à des intervalles réguliers tel que spécifié dans le plan de sauvegarde/récupération et archiver les résultats. Tester à la fois la récupération des données individuelles ainsi que la totalité des données. Les sauvegardes entreposées sur des sites extérieurs doivent faire l'objet de tests similaires

7.2 Sauvegarde des bases de données – Processus de routine

7.2.1 Les processus de sauvegarde dépendront du support utilisé. Idéalement, le système de sauvegarde devrait être automatisé et ne pas requérir une intervention humaine quotidienne de l'utilisateur (changement manuel du support de sauvegarde par exemple) afin de réduire les risques d'erreur

7.2.2 Procéder à des validations afin de garantir que la sauvegarde quotidienne a été complétée avec succès. Toute erreur de sauvegarde doit être analysée et corrigée de manière prioritaire.

7.3 Sauvegarde des bases de données – Fréquence

7.3.1 La fréquence est dépendante des besoins de récupération de la banque. La base de données devrait être sauvegardée quotidiennement durant la nuit. Une telle configuration limiterait la perte de données à une journée en cas de dommage ou de perte de données.

7.3.2 Le maintien d'un type d'archivage à l'aide des protocoles informatiques en cours est recommandé.

7.3.3 Entreposage hors site

a. Le RCBT recommande (au minimum) que des copies soient envoyées à l'extérieur une fois par mois, hebdomadairement si possible.

b. Le fournisseur de service doit être autorisé par l'institution d'accueil à gérer les données sensibles au lieu d'entreposage hors site.

7.4 Sauvegarde des bases de données – Plan de récupération

Mettre en place un plan de récupération pour la banque définissant les pertes de données acceptables. L'habilité à récupérer les données peut dépendre du système informatique et du SGBD utilisés.

7.5 Sauvegarde des bases de données – Vérification et validation des données récupérées

7.5.1 Développer un plan de tests pour s'assurer que les sauvegardes sont lisibles et contiennent des données valides.

7.5.2 Exécuter les tests tant pour la récupération intégrale de la base de données que pour la récupération des données individuelles sur une base trimestrielle.

8.0 RÉFÉRENCES, RÈGLEMENTS ET LIGNES DIRECTRICES

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 ANNEXES

Aucune

10.0 HISTORIQUE DES RÉVISIONS

Numéros des PNFs	Dates des modifications	Auteurs	Résumé des modifications
3.1.002 e1.0	2008	JdSH	Document initial
3.1.002 e1.0	May 2012	CMC	• Grammaire et mise en page • Retrait des définitions • Historique des révisions déplacé au bas du document • Mise à jour des liens pour les références • Mise à jour des références aux PNFs