Electronic Documents and Records

Electronic documents will be retained as if they were paper documents. Therefore, any electronic files that fall into one of the document types on the above schedule will be maintained for the appropriate amount of time. If a user has sufficient reason to keep an e-mail message, the message should be printed in hard copy and kept in the appropriate file or moved to an "archive" computer file folder. Backup and recovery methods will be tested on a regular basis. Passwords, usernames, and similar security identifications will have a file accessible by Governance Committee Chair.

1. **Emergency Planning.**

    a. The Organization's records will be stored in a safe, secure, and accessible manner. Documents and financial files that are essential to keeping the Organization operating in an emergency will be duplicated or backed up at least every week and maintained off-site.

2. **Document Destruction**

    a. The President is responsible for the ongoing process of identifying its records, which have met the required retention period, and overseeing their destruction. Destruction of financial and personnel-related documents will be accomplished by shredding.

    b. Document destruction will be suspended immediately, upon any indication of an official investigation or when a lawsuit is filed or appears imminent. Destruction will be reinstated upon conclusion of the investigation.

3. **Compliance**

    a. Failure on the part of employees to follow this policy can result in possible civil and criminal sanctions against the RCSRF and its employees and possible disciplinary action against responsible individuals. The President will periodically review these procedures with legal counsel or the organization's accountant to ensure that they are in compliance with new or revised regulations.