Financial Controls 9:
Financial Document Retention, Data Handling and Storage

As the title suggests, the subject of document care and maintenance extends beyond purely financial matters. It connects to mandates extending from privacy legislation as well as broader security concerns and general business practices.

Co-ops depend on their financial records to account for expenditures and receipts, whether internally or externally. In a world where transactions are often digital, controlling access to online accounts is also extremely important.

Co-ops need to draw clear lines of responsibility and determine who can access (financial) information and in what ways.

Federal legislation requires organizations to report data breaches to the Privacy Commissioner in certain cases: see section 10(1), *Personal Information Protection and Electronic Documents Act*

There is also provincial law protecting the personal information of co-op members and those applying to live at the co-op.

Canada Revenue Agency has provided an information circular on books and records retention: https://www.canada.ca/content/dam/cra-arc/formspubs/pub/ic78-10r5/ic78-10r5-10e.pdf

Recommendations

- Review the **job descriptions** for the Treasurer and Privacy Officer.
- Review related **policies** and written procedures, if they are present. If they aren't, develop new policies/procedures. (Examples include Document (Retention/Storage) Policies and Key Policies.)
- In general, keep financial records at least seven years securely. Pay attention to legally mandated retention schedules.
- Keep a **backup** of key records. A mix of onsite and offsite locations provides greater security.
- Maintain a regular **schedule for the disposal** of records (particularly important when concerning personal financial information).

  Note: documents impacting co-op operations may kept beyond standard timelines where that seems prudent.
- Consider the security and disposition of both virtual records and physical records.
- **Restrict access** to online passwords to authorized personnel.
- Online banking and other online financial services should be carried out only with **secure internet** connections: https, not http; avoid public wi-fi without a virtual private network.
- Develop **procedures for changing passwords** as needed (e.g. for example, on email accounts shared among board members: any change in board composition should trigger a change in passwords and authentication measures).

Indicator	Yes/ True	No/ False	Don't know
The Co-op has appropriate (e.g. locked, dry, organized) **storage facilities** for financial documents ☐ Hard copy / physical copies ☐ Digital copies			
The co-op has a **backup** of these financial records: ☐ On-site ☐ Off-site			
The co-op ensures **digital** copies are made of critical documents.			
These documents are not wholly in the hands of **external** organizations or a single employee.			
These documents are not wholly in the hands of a **single co-op member.**			
Online access to bank accounts is controlled (with passwords being reset when access changes).			
The co-op makes use of two- or multi-factor authentication (**MFA**) on financial accounts that allow for this authentication (unless a very clear rationale for non-adoption is made and regularly reviewed).			
The co-op employs a **3-2-1 strategy** for document storage (3 copies using 2 media types with 1 copy kept off-site).			

The co-op has a procedure to ensure **regular review** to determine which documents are to be kept and which are to be destroyed/deleted.			
The co-op has a procedure to safely and securely **destroy** documents flagged for deletion ("documents" in this case would extend to digital documents stored on non-paper physical media).			
Paper documents are (professionally) **cross-shredded**.			

Version dated: 2025-05-05