When Your Organization Goes Dormant or Closes: Securing Digital Assets

When an organization pauses operations or shuts down permanently, unmanaged digital accounts and data can become security and privacy liabilities. Sensitive files, domain names, and inactive accounts are common targets for compromise. The following checklist outlines essential steps to protect your organization, staff, and partners.

1. Designate a Digital Steward

Assign one person or a small, trusted team to oversee the shutdown process. Their responsibilities should include:

- Track all digital accounts and assets (email, domains, storage, social media, financial platforms, websites, etc.)
- Ensure accounts are properly secured, suspended, transferred, or deleted
- Maintain a final encrypted backup of critical information, on a separate hard drive if possible

2. Inventory and Classify Assets

List every platform and tool used:

- **Accounts**: Email, cloud storage, website hosting, social media, financial software, donor databases, collaboration tools
- **Hardware**: Laptops, phones, routers, external drives.

Classify each item as:

- To Keep/Transfer: Legal, financial, or historical value
- To Delete/Sanitize: No longer needed or contains sensitive data.

3. Secure or Delete Accounts

- Enable multi-factor authentication on all remaining accountsChange passwords and revoke access for departing staff and volunteers
- Remove or disable integrations with third-party apps.
- Delete or suspend inactive accounts—especially social media profiles and cloud storage—after archiving needed data.

4. Handle Data Responsibly

Follow a data minimization principle: keep only what you must.

- Encrypt and securely store retained records (e.g., legal, donor, or financial), ideally on a separate hard drive.
- Permanently delete personal or sensitive data that no longer serves a legal or operational purpose.
- Securely wipe devices before resale or recycling.

5. Preserve What Matters

Decide what should live on for transparency, historical value, or future relaunch.

- Archive public materials (press releases, reports, web content) in a read-only format.
- Maintain ownership of domain names and organizational email until they can safely expire or transfer.

6. Plan for Re-Activation (If Applicable)

If dormancy is temporary:

- Store credentials in an encrypted password manager accessible to the designated steward.
- Keep one secure email address active for password recovery and future communication.

7. Communicate Closure Securely

- Inform partners, funders, and audiences through official channels before accounts are deleted.
- Use encrypted or verified communication to notify staff and vendors.
- Post a clear closure message on your website or social accounts before archiving them.

Revision #11
Created 30 October 2025 19:23:26 by Josh
Updated 30 October 2025 20:08:14 by Josh