Organizations require procedures to manage day-to-day activities – in many cases, funders require them before agreeing to provide support. The following is an outline of what is required:

- Accessibility – making your technology accessible to staff, volunteers and clients with disabilities, if not required by law, certainly is considered best practice.
- Backup and Disaster Recovery – business resumption planning is imperative in the case of the following:
    - Physical disaster – fire, flood, earthquake
    - System Failure – server hard drive fails, workstation fails
    - Intrusion – server is "hacked" and destroyed, virus attacks and destroys files
- Acceptable Use – this policy should cover the following areas:
    - Who the policy applies to
    - Disciplinary procedures
    - General computer use
    - File management
    - Email usage
    - Email Signature conventions
    - Internet usage
    - Offensive material
    - Messaging/Chat
    - Purchasing Procedures
    - Online Purchasing
    - Physical Security
    - Confidential Data Protection
    - Passwords
    - Back-ups
    - Anti-virus/spam
    - Network Administration
    - Training
- Confidential Data Protection
    - What information is confidential? Names, addresses, etc.
    - Disclosure
    - What information is shared with partners, the public, etc.
- Health and Safety
    - Ergonomic standards
    - Options for staff – furniture, workstation set up, etc.