Risk Mitigation

This policy outlines the internal controls required to reduce financial risk, prevent fraud, and safeguard organizational integrity at Anything Helps. It includes expectations for staff conduct, financial oversight, physical security, and document retention. These practices support compliance with funding agreements and internal standards of accountability.

Definitions

- **Internal Control:** Processes and procedures to ensure the integrity of financial and accounting information, promote accountability, and prevent fraud.
- **Segregation of Duties:** Dividing responsibilities among different people to reduce the risk of error or inappropriate actions.
- **Physical Controls:** Security measures to protect physical assets and sensitive information.

Segregation of Duties

Accounting responsibilities are divided among at least three people. Monthly financial statements are reviewed by more than one staff member. When a transaction appears questionable, it must be documented and resolved by a person with the authority to approve it. Employees are expected to keep their tasks transparent and accessible. No one may restrict others from viewing or reviewing their work. Staff must also take regular time off, during which others are assigned to review and perform their duties to ensure continuity and reduce risk.

Personnel Risk Controls

Staff are screened prior to hire, including reference checks. Any employee with access to financial systems or client funds is covered by a fidelity bond. During employment, team members may be evaluated for potential risk factors such as major lifestyle changes, financial distress, or substance use. These reviews are not punitive but serve to protect the organization and ensure early intervention when appropriate.

Physical and Digital Safeguards

Sensitive materials and assets are protected through both physical and digital controls. Blank checks and signature stamps are locked in a secure location. Inventory and physical assets are stored with limited access. Customer credit card data is never retained or stored. Digital records are backed up regularly to secure offsite systems. Passwords are reviewed and updated frequently and are accessible only to staff with a clear need. Insurance coverage is reviewed each year to confirm that risk areas are adequately protected.

Retention of Financial and Organizational Records

Records are retained based on their operational value and compliance requirements:

- Items retained for **2 years** include: *bank reconciliations, correspondence, and duplicate deposit slips.*
- Items retained for **3 years** include: *bank statements, employment applications, expired insurance policies, and internal audit reports.*
- Items retained for **7 years** include: *accounts payable schedules, expired contracts, mortgages and leases, expense breakdowns, inventory records, vendor and customer invoices, payroll records and timesheets, personnel files for former staff, and tax withholding documents.*
- Items retained **permanently** include: *audit reports, checks, active contracts, legal correspondence, deeds and bills of sale, depreciation schedules, year-end financials, governance documents (including bylaws, charters, and minute books), current insurance policies, intellectual property filings (trademarks, copyrights, patents), pension and retirement records, and tax returns.*

If a legal case, audit, or investigation is pending or expected, *all related records*—regardless of their original retention schedule—*must be preserved* until resolution is formally documented.

Compliance and Oversight

The Executive Director is responsible for oversight and enforcement of this SOP. The Lead Administrator ensures documentation is current, staff are trained on these protocols, and any exceptions are approved in writing. Internal reviews of compliance will be conducted annually or in response to suspected breaches. Records of these reviews must be retained and made available upon request during audits or monitoring visits.