NONPROFIT CYBERSECURITY BASELINE CHECKLIST

Check the controls behind the work

A 30-minute leadership review for nonprofits, human-services and behavioral-health organizations. Complete it with the person responsible for technology management.

> Status key: Yes = current evidence exists; Partial = incomplete coverage; No = missing; Unknown = unverified; N/A = documented reason. Do not mark Yes based only on a vendor promise. Use this to identify questions, not to certify security.

Organization / review date / business lead / technology contact

A named person follows through on technology risks --

Evidence: current responsibility list, escalation route and a record of open actions.

User and administrator access is protected by MFA --

Evidence: enforcement report and documented exceptions. Give privileged and remote access particular attention. [1]

Administrative access is limited and separate --

Evidence: role list, separate admin accounts and a tested emergency-access procedure.

Departures and role changes remove unneeded access --

Evidence: a recent completed checklist covering accounts, sessions, apps, devices and transferred work.

Staff can report suspicious messages or account activity --

Evidence: a simple reporting route and training that fits frontline, shift and remote staff.

02 / DEVICES AND EMAIL

Follow the work beyond the office

Check laptops, shared workstations, mobile use and remote access that support program delivery. A control installed on office PCs may not cover all staff workflows.

Devices reaching important systems are inventoried --

Evidence: device list, assigned contact, support status and a process for lost or retired equipment.

Updates and endpoint protection are monitored --

Evidence: coverage reports, alert response and named responsibility for failed updates or exclusions.

Portable devices have verified encryption --

Evidence: encryption status and securely held recovery keys that an authorized administrator can retrieve.

Routine users do not have unnecessary local admin rights --

Evidence: local administrator review and a workable route for approved software installation.

Remote and personal-device access follows a policy --

Evidence: approved access method, sign-in controls and rules for sensitive information on unmanaged devices.

Email authentication and filtering are checked --

Evidence: domain authentication results, filtering coverage and a process for reviewing legitimate messages that are incorrectly blocked.

Payment and sensitive-data requests get independent checks --

Evidence: a known-number callback process for changed banking instructions and staff guidance for unusual requests.

Important exception / affected program / responsible contact

03 / RECOVERY AND RESPONSE

Prepare for the interruption

Choose a critical service and trace what happens if its application, identity service or vendor becomes unavailable. [2]

Backup coverage includes the data staff actually use

Evidence: a protected-system list including cloud and vendor-hosted data, recovery windows and exclusions.

--

A restore test proves a useful staff task can be completed

Evidence: measured result, staff validation and corrective actions; a green backup report alone is insufficient.

--

Shared files and vendor access are reviewed

Evidence: permission reviews, named approvers, guest expiry decisions and a current vendor register.

--

Incident contacts and decision authority are documented

Evidence: incident lead and deputy, provider and insurer contacts, and who can authorize containment or external communication.

--

Staff have an approved downtime process

Evidence: accessible instructions for critical work, secure temporary records and later reconciliation.

--

Policies and insurance answers match current practice

Evidence: approved policies and supporting reports. Have the responsible adviser confirm actual policy or contractual requirements.

--

Critical service / biggest unverified dependency / next evidence request

04 / EVIDENCE AND ACTION

Close the highest-impact gaps

Select three actions based on service impact and exposure. Keep a missing control, a missing document and an unknown answer distinct.

Action 1 / responsible person / due date / proof needed

Action 2 / responsible person / due date / proof needed

Action 3 / responsible person / due date / proof needed

Next review date / escalation contact / evidence folder

Useful evidence pack: access review, device coverage report, latest recovery-test result, incident contact list, key vendor contacts and the current action register. Restrict access to these records; do not attach passwords or participant data.

Reference guidance

[1] Microsoft: Multifactor authentication overview

[2] NIST: Cybersecurity Framework 2.0 - Small Business Quick-Start Guide

This is a starting checklist, not an audit, complete risk assessment, insurance determination or compliance certification. Recommendations should be adapted to your services and obligations. Reviewed September 8, 2026.