SAMPLE REPORT. "Riverside Community Center" is a fictional organization. This document demonstrates the format, depth, and plain-English style of every Coeus Tech checkup deliverable. Client reports are based on a real remote review of your environment.

IT Security Checkup

Riverside Community Center · 12 staff · Microsoft 365 + mixed devices · Remote review

The Short Version

Your day-to-day systems work, and your team clearly keeps things running with very little. But three findings need attention soon: **anyone who steals one staff password can read that person's email and send as your organization (no MFA)**, **your donor spreadsheet exists in exactly one place**, and **two former staff members still have working accounts**. All three are inexpensive to fix — the total recommended remediation below is under $700 and about a week of calendar time. Everything else on the scorecard is in reasonable shape for an organization your size.

Scorecard

AREA	STATUS	ONE-LINE SUMMARY
Email security	Action needed	No MFA on any account; no protection against look-alike phishing
Accounts & access	Action needed	2 former-staff accounts still active; shared password for the office PC
Backup & recovery	Needs work	Donor and finance files have no second copy anywhere
Devices	Needs work	Mixed personal/org laptops; antivirus present but unmanaged
Network & Wi-Fi	Needs work	Guests, staff, and office systems share one network
Microsoft 365 setup	Good	Licensed correctly; email on your own domain; no overspend found
Website & domain	Good	Domain auto-renews; site hosted and SSL valid

What We Found (in plain English)

1. One stolen password = full access (no multi-factor authentication)

Risk: High · Fix effort: Low · Affects: all 12 staff accounts

Right now, an email password is the only thing between an attacker and a staff inbox. Phishing kits harvest these passwords automatically — it is the #1 way small organizations get compromised, and a compromised inbox can email your donors and partners *as you*. MFA (the "code on your phone" second step) blocks over 99% of these attacks. **The fix:** enable MFA for all accounts with a staged rollout — announcement email, a one-page setup guide for staff, then enforcement — so nobody gets locked out mid-week.

2. Two former employees can still log in

Risk: High · Fix effort: Trivial · Affects: email, files, donor data

Two accounts belonging to staff who left in 2024 and 2025 are still active, with full access to email and shared files. Even if you trust both people completely, their passwords may already be circulating in breach databases. **The fix:** disable both accounts, convert mailboxes to shared (so history is kept), and adopt a 15-minute offboarding checklist for the future — included with this report.

3. Your donor records exist in exactly one place

Risk: Medium today, severe the day it happens · Fix effort: Low

The donor spreadsheet and finance files live only on the office PC's local drive. One failed hard drive, ransomware infection, or theft and they're gone — there is no second copy. **The fix:** move working files into your existing Microsoft 365 storage (already paid for — OneDrive/SharePoint), which adds version history and ransomware rollback, plus one automated offline backup of the critical folder.

4. Guests share the network with your office systems

Risk: Medium · Fix effort: Low-Medium (config only, no new hardware)

Visitors who get the Wi-Fi password land on the same network as the office PC holding your finance files. Your existing router supports a separated guest network — it has simply never been configured. **The fix:** a guest network with isolation turned on, done remotely via your router's management page, with zero new equipment.

5. Your Microsoft 365 licensing is actually right (no action)

Good news

You're on the correct license tier for your size, you're not paying for unused seats, and email runs on your own domain. We checked for the common overspend patterns (duplicate subscriptions, premium tiers nobody uses) and found none. Whoever set this up did it properly.

Recommended Fix Plan (priced, prioritized)

#	FIX	WHY FIRST	FIXED PRICE	TIMELINE
1	Disable former-staff accounts + offboarding checklist	Open door, trivial to close	Included free with this report	Same day
2	MFA rollout for all 12 staff (announcement, guide, enforcement, lockout support week)	Blocks the #1 attack on small orgs	$300	1 week
3	Donor/finance files to M365 storage + automated backup	Eliminates the single point of total loss	$200	2–3 days
4	Guest Wi-Fi separation (remote router configuration)	Walls off visitors from office systems	$150	1 day
5	Managed antivirus (Defender) on org laptops	Visibility when something does get through	quoted after device count confirmed	—

Everything above (items 2–4): $650 flat. No retainer required. Each item is delivered with plain-English documentation of what changed and why, so any future IT provider can pick up where we left off. Ongoing "IT on call" support is available afterward ($150–300/month) but never required — the fixes stand on their own.

How This Review Was Done

- Remote, read-only review of the Microsoft 365 admin environment (accounts, licenses, security settings, mail protection)
- DNS and email-authentication check (SPF, DKIM, DMARC) from public records
- Written questionnaire with the office administrator — no meetings required
- No changes were made to any system during the review

Questions?

Everything happens by email: **matt@coeustech.net**. You'll always get a plain-English answer, usually same-day.