Sector Risk Full Guide (Education & Nonprofit Edition)

How small orgs reduce attacks and pass audits—without buying more tools.

1) What attackers target in small orgs

Email/payment workflows, public calendars, shared inboxes, volunteer devices. Quick mitigation: enforce MFA, remove shared passwords, limit mailbox rules.

2) Human-first controls auditors look for

Annual training + quarterly refreshers. Incident reporting steps and acceptable use basics. Evidence to keep: training roster, certificates, policy, annual summary page.

3) 7 quick wins (checklist)

1. MFA on email & key apps.
2. Password manager or minimum password rules.
3. Phishing report button/process.
4. Device lock + auto-update enabled.
5. Off-boarding checklist (accounts, keys, shared drives).
6. Vendor/security review folder (SOC2, insurance, policy, roster).
7. Quarterly 10-minute refresher schedule.

4) Insurance & grant language—what it means

“Security awareness training” = real training + proof of completion.
“Incident response” = who you call + a 1-page action plan.
“Reasonable controls” = MFA, updates, access limits, documented reviews.

5) Templates (plain-English)

Training Log: Name | Role | Module | Date | Certificate Y/N
Evidence Pack index: Policy (PDF), Training Roster (CSV/PDF), Certificates (PDF), Annual Summary (1-pager), Vendor Review Docs.
Board/Donor Summary: What we did, Who was covered, Dates, Next steps.

6) Rollout in two weeks

Week 1: Send training, set MFA baseline, publish policy.
Week 2: Collect roster/certificates, create evidence pack, schedule next refresher.

Closing CTA: Need a turnkey version with certificates and an evidence pack? Secure Habits gets you audit-ready in two weeks.