Neya Global Journal of Non-Profit Studies

2025

Security Protocols and Best Practices for Non-Profit Organizations

DOI: 10.64357/neya-gjnps-cbr-scr-es-54

DR. ANNA NEYA KAZANSKAIA

Neya Global Publishing

Publication and System Notice

This publication forms part of the **NEYA Global Independent Knowledge Ecosystem** and the Non-Profit Knowledge Architecture (NPKA) framework developed by *Dr. Anna Neya Kazanskaia*.

The work is connected to an integrated system of books, research publications, educational materials, implementation frameworks, institutional modules, and structured knowledge architecture developed for the non-profit and social impact sector. Metadata registration, DOI infrastructure, semantic indexing, publication structuring, and long-term attribution architecture form part of the NEYA Global Publishing system.

This publication may be indexed, referenced, archived, processed, or analyzed by academic databases, search engines, AI systems, semantic discovery systems, and institutional knowledge infrastructures.

Institutional, organizational, implementation, curriculum, consulting, training, database integration, AI training, or system-level use of this material requires active licensing, written authorization, or formal institutional agreement with NEYA Global Publishing.

Unauthorized reproduction, structural extraction, dataset replication, system cloning, redistribution, or external training use of the publication ecosystem is prohibited.

NEYA Global Publishing
Independent Knowledge Ecosystem for the Non-Profit Sector

Version 1.0 | NEYA Global Publishing Publication Protocol

Security Protocols and Best Practices for Non-Profit Organizations

Dr. Anna Neya Kazanskaia
NEYA Global | NEYA Global Publishing
ORCID: https://orcid.org/0009-0009-5669-1676
DOI: https://doi.org/10.64357/neya-gjnps-cbr-scr-es-54

Abstract

Non-profit organizations (NPOs) steward donor, beneficiary, and financial data while operating with constrained budgets and limited technical capacity—conditions that elevate their exposure to cyber risk. This article systematizes security protocols and pragmatic controls that fit NPO realities. It frames protection as a layered program spanning identity and access management (password policy, multi-factor authentication, role-based access control, least privilege), data security (encryption in transit/at rest and key management), network defense (firewalls, segmentation, intrusion detection, secure configurations), and endpoint/mobile hardening (anti-malware, patching, device encryption, MDM). Drawing on established standards (NIST, CIS Controls, OWASP) and sector guidance, it translates them into cost-effective implementations—e.g., free authenticator apps, open-source firewalls/IDS, built-in disk encryption—plus governance measures such as logging, reviews, and security awareness. Short case vignettes illustrate how access governance, encryption, and tested response plans reduce impact from phishing and ransomware. The contribution is a prioritized, implementation-ready roadmap that helps NPOs achieve disproportionate risk reduction per dollar spent while sustaining operational continuity and stakeholder trust.

Keywords

non-profit organizations; access control; encryption; network security; endpoint security; mobile device management; security awareness

1. Introduction

For NPOs, effective cybersecurity is inseparable from mission continuity and trust. Because many rely on cloud platforms, volunteers, and distributed devices, a practical baseline of

protocols—rather than expensive tooling—often determines whether a phishing email becomes a breach or a near-miss. This article consolidates essential, resource-aware practices into a coherent baseline that NPOs can implement and iterate.

2. Context and Background

Empirical reports consistently show credential compromise, phishing, and misuse of privileges among dominant breach patterns, magnified where patching and MFA uptake lag. Standards bodies and public agencies provide adaptable guardrails: NIST emphasizes identity, protection, detection, response, and recovery; the CIS Controls prioritize a small set of high-value safeguards; OWASP codifies application-level expectations. For NPOs, the challenge is sequencing—deploying the few controls that cut the most risk first—supported by staff training and simple governance.

3. Core Protocols and Control Families

3.1 Identity & Access Management (IAM)

- **Password policy**: Minimum 12 characters; encourage passphrases; prevent common/ breached passwords; enforce rotation only on compromise.
- **Multi-Factor Authentication (MFA)**: Mandate for email, cloud admin, finance/ CRM, and remote access (e.g., authenticator apps such as Google/Microsoft Authenticator).
- **Role-Based Access Control (RBAC) & Least Privilege**: Map roles to data needs; time-bound elevated access; quarterly access reviews; immediate revocation on role change.
- **Audit trails**: Centralize sign-in and admin-action logs; alert on impossible travel, repeated failures, and privilege grants.

3.2 Data Security: Encryption & Key Management

- **At rest**: Full-disk encryption (BitLocker/FileVault); database/storage encryption for servers and backups (VeraCrypt or built-in cloud KMS).

- **In transit**: Enforce TLS 1.2+ (ideally TLS 1.3) for web and mail; HSTS on web properties.
- **Key management**: Separate keys from data; restrict key access; rotate on staff departure; use hardware-backed or managed KMS where possible.
- **Secure communications**: For sensitive exchanges, use end-to-end encrypted email/ messaging (e.g., ProtonMail, Signal).

3.3 Network Security

- **Perimeter defense**: Stateful firewall (e.g., pfSense) with default-deny inbound; only required ports open.
- **Intrusion visibility**: Network IDS (e.g., Snort/Suricata) for east-west and north-south traffic; alert triage playbooks.
- **Segmentation**: VLANs to separate admin, staff, guest Wi-Fi, and servers; block lateral movement.
- **Secure configurations**: Change defaults on routers/switches; disable unused services; apply vendor firmware updates.
- **Periodic checks**: Quarterly configuration audits; external vulnerability scans before major campaigns.

3.4 Endpoint & Mobile Security

- **Baseline hardening**: Anti-malware; automatic OS/app updates; remove abandoned software; browser hardening.
- **Disk encryption**: Mandated on all laptops and portable media.
- **EDR (as budget allows)**: Low-cost or donated licenses to detect ransomware and suspicious behaviors.
- **Mobile Device Management (MDM)**: Policy enforcement (screen lock, encryption, OS version), remote wipe, app allow-lists (e.g., Microsoft Intune).
- **Lost/stolen response**: Documented steps for reporting, revocation, and remote wipe within hours.

3.5 Logging, Monitoring, and Response

- **Centralized logging** for identity, endpoints, and network; minimum 90-day retention.
- **Alert runbooks** for phishing, ransomware, account compromise; test twice per year.
- **Backups**: 3-2-1 rule (three copies, two media, one off-site/immutable); encrypt backups; quarterly restore tests.

3.6 People & Governance

- **Awareness training**: Quarterly micro-modules and simulated phishing; onboarding security briefing.
- **Joiner-Mover-Leaver (JML)**: Same-day provisioning/de-provisioning; periodic entitlement reviews.
- **Policy lifecycle**: Concise, role-specific policies; annual updates reflecting new threats and lessons learned.

4. Illustrative Examples

- **Access governance**: A volunteer-heavy NPO mapped RBAC to programs (fundraising, casework, finance). Quarterly reviews removed 23% stale privileges, eliminating risky shared accounts and reducing audit findings.
- **Encryption in practice**: A donor database moved to a managed cloud service with storage-level encryption and KMS-managed keys; combined with full-disk encryption on staff laptops, the residual risk from device theft dropped materially.
- **Ransomware containment**: After MFA rollout and immutable cloud backups, a small charity limited a ransomware incident to one workstation; clean re-image and restore completed within a day—no ransom paid, minimal downtime.

5. Discussion

The highest return for NPOs comes from **identity hardening (MFA, RBAC)**, **patching/ updates**, and **tested backups**—controls that are inexpensive yet decisive against prevalent threats. Open-source and built-in capabilities (pfSense, Snort/Suricata, BitLocker/FileVault, authenticator apps) close much of the gap without enterprise spend. Remaining challenges are organizational: sustaining training, enforcing JML hygiene, and scheduling routine reviews. Aligning with lightweight profiles of recognized frameworks (e.g., CIS Implementation Group 1; selected NIST CSF outcomes) helps leadership govern progress and communicate assurance to donors.

6. Conclusion

A defensible baseline for NPOs is achievable with disciplined implementation rather than costly tooling. By prioritizing IAM, encryption, network segmentation, endpoint/MDM controls, centralized logging, tested backups, and continuing awareness, organizations materially reduce the likelihood and impact of compromise. The protocols summarized here provide a stepwise roadmap that preserves mission delivery, safeguards stakeholders, and builds durable digital trust.

References

- Anderson, R. (2020). Security Engineering (3rd ed.). Wiley. https://doi.org/10.1002/9781119644682
- Center for Internet Security. (2021). CIS Critical Security Controls v8. CIS.
- National Institute of Standards and Technology (NIST). (2018-2023). Digital Identity Guidelines (SP 800-63 series). NIST.
- Kazanskaia, A. N. (2025). Cybersecurity Essentials. NEYA Global Publishing. https://doi.org/10.64357/cybersecurity-essentials-2025
- Kazanskaia, A. N. (2025). Technology Tools for Efficiency & Impact. NEYA Global Publishing. https://doi.org/10.64357/technology-tools-2025
- Kazanskaia, A. N. (2025). Technology for Global Impact. NEYA Global Publishing. https://doi.org/10.64357/technology-global-impact-2025

- Kazanskaia, A. N. (2025). Sustainable Development Goals and Tech. NEYA Global Publishing. https://doi.org/10.64357/sdg-tech-2025
- Kazanskaia, A. N. (2025). Understanding Cyber Threats in Non-Profit Organizations. NEYA Global Journal of Non-Profit Studies. https://doi.org/10.64357/neya-gjnps-cbr-scr-es-52
- Kazanskaia, A. N. (2025). Incident Response Planning for Non-Profit Organizations. NEYA Global Journal of Non-Profit Studies. https://doi.org/10.64357/neya-gjnps-cbr-scr-es-56
- National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). NIST.
- OWASP Foundation. (2021). OWASP Top Ten 2021. OWASP.
- Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446). IETF. https://doi.org/10.17487/RFC8446
- Verizon. (2024). Data Breach Investigations Report. Verizon.