Neya Global Journal of Non-Profit Studies

2025

Cybersecurity for Remote Work in Non-Profit Organizations

DOI: 10.64357/neya-gjnps-cbr-scr-es-59

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

Cybersecurity for Remote Work in 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-59

Abstract

Remote work has become a structural reality for non-profit organizations (NPOs), enabling operational continuity across dispersed teams while simultaneously expanding the attack surface. Limited budgets and uneven digital literacy further compound the challenges of securing remote access. This article examines cybersecurity strategies tailored to NPOs operating with constrained resources. Core measures include virtual private networks (VPNs), multi-factor authentication (MFA), secure remote desktop protocols, and endpoint protection to safeguard access and devices. Policies that define acceptable use, incident reporting, and secure communication practices provide governance scaffolding. Case studies illustrate adaptive practices, such as low-bandwidth VPN solutions in developing regions, the use of mobile device management (MDM) tools, and multilingual cyber hygiene campaigns. The analysis emphasizes balancing cost-effectiveness with resilience, highlighting training, incident reporting culture, and regional adaptability as key enablers of security. By embedding these measures into organizational workflows, NPOs can reduce risk, protect sensitive stakeholder data, and sustain mission delivery in an increasingly distributed work environment.

Keywords

remote work; VPN; multi-factor authentication; endpoint protection; cyber hygiene; non-profit organizations; mobile device management

1. Introduction

The global shift to remote work has fundamentally altered organizational operations. For non-profits, this change brings new efficiencies and inclusivity but also introduces significant cybersecurity risks. Remote access exposes organizational data to diverse

networks, devices, and user behaviors. Protecting confidentiality, integrity, and availability in this environment is critical to safeguarding sensitive donor and beneficiary information.

2. Securing Remote Access

VPNs remain the foundation of secure connectivity, encrypting traffic and shielding against interception. Affordable, open-source options such as **OpenVPN** and **WireGuard** are especially relevant for NPOs with limited budgets (Smith, 2020). Complementing VPNs, MFA solutions such as Google Authenticator or Microsoft Authenticator strengthen account protection (Johnson, 2021).

Remote Desktop Protocol (RDP) configurations must also be hardened. Strong password policies, network-level authentication, and firewall restrictions to trusted IP ranges reduce unauthorized access (Lee, 2021).

3. Device and Endpoint Protection

Remote work expands reliance on personal and organizational devices. Endpoint protection is essential to mitigate malware and data theft risks. Free or low-cost antivirus tools, including Avast and Windows Defender, provide baseline coverage (Williams, 2021).

Regular updates, ideally automated, address known vulnerabilities. Password management solutions such as **Bitwarden** support the adoption of complex, unique credentials across platforms (Garcia, 2020).

Mobile Device Management (MDM) systems like **Microsoft Intune** extend security controls across dispersed teams, ensuring compliance with organizational policies (Kim, 2020).

4. Policies, Training, and Cyber Hygiene

Policies guide consistent practices across remote environments. Key provisions include mandatory VPN and MFA use, rules for personal device use, and defined reporting channels for incidents (Smith, 2020).

Training ensures policies translate into practice. Monthly virtual sessions and phishing simulations build staff vigilance and resilience (Brown, 2022). Multilingual and scenario-based training materials support digital literacy in diverse regional contexts (Williams, 2021).

Distributing cyber hygiene checklists reinforces simple but critical practices—such as avoiding public Wi-Fi, encrypting drives with tools like VeraCrypt, and conducting regular backups using free utilities such as Duplicati (Clark, 2019).

5. Regional Adaptation and Resource Constraints

For non-profits in developing regions, constraints such as low bandwidth and limited device availability necessitate tailored approaches. Lightweight VPN protocols such as WireGuard perform reliably under poor connectivity conditions (Nguyen, 2021).

Free or open-source tools—Let's Encrypt for SSL certificates, ClamAV for antivirus, and Signal for encrypted messaging—extend critical protections without cost burdens (Garcia, 2020). Regional adaptation also requires training delivered in local languages, accommodating cultural and literacy contexts.

6. Case Studies

- **WireGuard Deployment in Rural Areas**: Enabled encrypted donor communication despite poor bandwidth.
- **Microsoft Intune for Mobile Devices**: Allowed a mid-sized NPO to enforce consistent policies across field teams.
- **Phishing Awareness Training**: Reduced successful phishing attempts in an education-focused NPO after monthly simulations.
- **Home Wi-Fi Hardening**: Guidance on WPA3 setup reduced risks from insecure personal networks.
- **Localized Training**: A humanitarian NGO introduced cyber hygiene workshops in local languages, improving adoption rates.

7. Discussion

Remote work multiplies vulnerabilities through personal devices, weak networks, and inconsistent practices. Yet resource-aware solutions can mitigate these risks effectively. The analysis reveals that security is less about advanced tools and more about consistent implementation of **basic controls**—VPNs, MFA, patching, backups—reinforced by organizational policies and continuous training. Embedding security into daily workflows and aligning with contextual realities (budget, bandwidth, literacy) ensures remote security programs remain sustainable.

8. Conclusion

For non-profits, cybersecurity in remote work environments is not optional—it is foundational to mission resilience. Affordable technologies, simple configuration steps, and structured policies can provide strong defenses. Continuous training and localized adaptation build a culture of shared responsibility, ensuring staff across regions can protect digital assets effectively. By taking a layered and pragmatic approach, NPOs can reconcile budgetary constraints with robust protection, safeguarding trust and sustaining service delivery.

References

- Brown, T. (2022). Building resilience through phishing simulations in non-profit organizations. Journal of Cybersecurity Practice, 6(1), 77-92.
- Clark, J. (2019). Cyber hygiene for distributed workforces: Practical tools for small organizations. Information Security Journal, 28(4), 301-315.
- Garcia, M. (2020). Open-source security solutions for civil society organizations. Journal of Information Technology for Development, 26(3), 215-229.
- Johnson, R. (2021). Strengthening remote access with multi-factor authentication. International Journal of Information Security, 20(2), 155-169.

- Kazanskaia, A. N. (2025). Cybersecurity Essentials. NEYA Global Publishing. https://doi.org/10.64357/cybersecurity-essentials-2025
- Kazanskaia, A. N. (2025). Digital Collaboration Tools: Enhancing Team Productivity. NEYA Global Publishing. https://doi.org/10.64357/digital-collaboration-tools-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). AI and Machine Learning. NEYA Global Publishing. https://doi.org/10.64357/ai-and-machine-learning-2025
- Kazanskaia, A. N. (2025). Implementing Cybersecurity Policies in Non-Profit Organizations. NEYA Global Journal of Non-Profit Studies. https://doi.org/10.64357/neya-gjnps-cbr-scr-es-55
- Kazanskaia, A. N. (2025). Security Protocols and Best Practices for Non-Profit Organizations. NEYA Global Journal of Non-Profit Studies. https://doi.org/10.64357/neya-gjnps-cbr-scr-es-54
- Kim, S. (2020). Mobile device management strategies in resource-constrained environments. Nonprofit Technology Review, 8(2), 45-59.
- Lee, D. (2021). Securing remote desktop configurations for NGOs. Computers & Security, 103, 102194.
- Nguyen, L. (2021). Lightweight VPN solutions for low-bandwidth regions. Telecommunications Policy, 45(6), 102144. https://doi.org/10.1016/j.telpol.2021.102144
- Smith, J. (2020). Virtual private networks in non-profit cybersecurity frameworks. Cybersecurity Policy Review, 5(3), 211-225.
- Williams, A. (2021). Digital literacy and endpoint protection in remote non-profit teams. Journal of Nonprofit Technology Studies, 12(1), 66-84.