center4

Non-Profit Technology Policy Workbook

Center4 Nonprofit Technology Policy Workbook *(2026 Edition)*

A Modern, Practical Policy Framework for Secure, Ethical, and Resilient Nonprofit Operations

A free, vendor-neutral workbook for nonprofit boards, executives, and operations leaders

---

About This Workbook

Technology risk is now **organizational risk**. Since the original 2020 workbook was published, nonprofits have experienced: - A dramatic rise in ransomware and phishing attacks - Widespread remote and hybrid work - Increased regulatory scrutiny around privacy and data handling - Greater reliance on cloud platforms, vendors, and business associates

This **Center4 Nonprofit Technology Policy Workbook (2026 Edition)** is a **fully rewritten, expanded, and modernized replacement** for the original Nonprofit Technology Policy Workbook fileciteturn16file0.

All references to **TechImpact**, sponsors, advertisements, services, websites, conferences, and affiliated organizations have been **completely removed**.

This workbook is designed to: - Help nonprofits establish **clear, defensible technology policies** - Support board fiduciary and oversight responsibilities - Align IT practices with modern security, privacy, and compliance expectations - Provide **practical policy templates and checklists**, not vendor marketing

---

How to Use This Workbook

This workbook can be used in three ways: 1. **Policy Creation** – for organizations without formal technology policies 2. **Policy Refresh** – to update outdated policies written before 2023 3. **Board & Audit Support** – as documentation of due diligence and governance

You do **not** need to implement every policy at once. Start with high-risk areas and build over time.

Core Technology Policies Every Nonprofit Should Have (2026)

At minimum, nonprofits should maintain written policies covering: - Acceptable Use of Technology - Bring Your Own Device (BYOD) - Data Classification & Handling - Information

Security - Incident Response - Disaster Recovery & Business Continuity - Vendor & Third-Party Risk

This workbook walks through each area step by step.

SECTION 1: Acceptable Use Policy (AUP)

Purpose

Defines how staff, volunteers, contractors, and board members may use organizational technology and data.

2026 Enhancements

- Explicit coverage of cloud services and SaaS tools
- AI tool usage expectations (e.g., generative AI, transcription, analytics)
- Social media and collaboration platforms

Key Elements to Define

- Who the policy applies to
- Covered devices, systems, and accounts
- Ownership of data and work product
- Monitoring expectations
- Consequences for violations

Center4 Recommendation: Ensure the AUP explicitly includes *remote access* and *home networks*.

SECTION 2: Bring Your Own Device (BYOD) Policy

Purpose

Balances convenience, cost savings, and security when personal devices are used for work.

2026 Enhancements

- Mobile Device Management (MDM) expectations
- Encryption and device lock requirements
- Remote wipe authorization
- Reimbursement and stipend clarity

Required Policy Decisions

- Approved device types
- Security configuration requirements
- Lost or stolen device reporting timelines
- Support boundaries for IT teams

SECTION 3: Data Classification & Handling Policy

Purpose

Ensures sensitive data is handled appropriately based on risk.

Data Categories

- **Confidential** (PII, PHI, donor data)
- **Essential** (financials, operations)
- **Public** (marketing, reports)

2026 Enhancements

- Data minimization principles
- Retention and destruction timelines
- Encryption standards for data at rest and in transit

SECTION 4: Information Security Policy

Purpose

Defines baseline security expectations across systems and users.

2026 Minimum Standards

- Multi-Factor Authentication (MFA)
- Password manager usage
- Endpoint protection
- Email filtering and phishing awareness training
- Role-based access control (least privilege)

Center4 Insight: MFA is no longer optional—it is a baseline expectation.

SECTION 5: Vendor, Third-Party & Business Associate Policy

Purpose

Addresses risk introduced by external providers.

Required Coverage

- Vendor due diligence process
- Data access limitations
- Security expectations
- Incident notification requirements

Business Associate Agreements (BAAs)

Nonprofits handling regulated data (HIPAA, FERPA, etc.) should require BAAs from applicable vendors.

SECTION 6: Incident Response Policy

Purpose

Defines how the organization responds to security incidents.

Incident Types

- Phishing or credential compromise
- Ransomware or malware
- Data exposure or breach

2026 Enhancements

- Incident severity classification
- Regulatory notification timelines
- Cyber insurance coordination
- Law enforcement engagement criteria

SECTION 7: Disaster Recovery & Business Continuity Policy

Purpose

Ensures continuity of mission-critical services.

Required Components

- Critical system inventory
- Backup frequency and testing
- Recovery time objectives (RTO)
- Alternative operating procedures

Center4 Recommendation: Test disaster recovery annually—assumptions fail under stress.

SECTION 8: Privacy & Compliance Policies (Expanded)

Nonprofits should maintain policies aligned with applicable regulations:

- **HIPAA & PHI** (health services)
- **FERPA** (education records)
- **PCI-DSS** (credit card handling)
- **State privacy laws** (NY SHIELD Act, CCPA/CPRA where applicable)

Policies should define: - Data access controls - Breach notification processes - Training requirements

---

SECTION 9: Emerging & New Policy Areas (2026)

AI & Automation Usage Policy

- Approved vs prohibited uses
- Data input restrictions
- Human review requirements

Remote Work Security Policy

- Home network requirements
- VPN or secure access standards

- Physical security expectations

Cyber Insurance Policy

- Coverage scope
- Claim procedures
- Required security controls

SECTION 10: Policy Templates & Document Checklist

Nonprofits should maintain templates for:

- Acceptable Use Policy
- BYOD Policy
- Data Classification Policy
- Information Security Policy
- Incident Response Plan
- Disaster Recovery Plan
- Vendor Risk Assessment Template
- Business Associate Agreement (BAA)
- Confidentiality & NDA Agreements
- Employee & Volunteer Technology Acknowledgment

Board Oversight & Governance Guidance

Boards should: - Review technology policies annually - Document approvals in meeting minutes - Ensure alignment with risk appetite - Confirm training completion

Technology governance is a **fiduciary responsibility**.

Conclusion

Strong technology policies do not eliminate risk—but they **demonstrate diligence, preparedness, and leadership**. In today’s threat environment, nonprofits must treat technology governance as mission-critical.

This workbook is intended to be adapted, reviewed regularly, and used as a living document.

Center4 provides free, practical, vendor-neutral resources to help nonprofit organizations strengthen governance, reduce risk, and operate with confidence in a digital-first world.