CSNP
CYBERSECURITY NON-PROFIT

Nonprofit Data Protection Guide

Essential cybersecurity strategies for protecting your mission-critical data on any budget

CHAPTER 1

Why Nonprofits Are Prime Targets

Cybercriminals increasingly target nonprofit organizations, recognizing them as vulnerable entry points to valuable data. Many nonprofits operate with limited IT resources and cybersecurity expertise, making them attractive targets for ransomware attacks, data breaches, and financial fraud.

The stakes are high: a single breach can compromise donor trust, disrupt operations, and damage your organization's reputation for years to come.

43%

Nonprofits Breached

Nearly half of nonprofits experienced a cyberattack in recent years

60%

Lack Basic Protection

Don't have adequate cybersecurity measures in place

$200K

Average Breach Cost

Financial impact including recovery and lost donations

CHAPTER 2

Protecting Your Donor Data

Donor information is your organization's most valuable asset and carries significant responsibility. Implementing robust protection measures builds trust and ensures compliance with data protection regulations.

Encryption First

Encrypt all donor data both in transit and at rest using industry-standard protocols. Use secure payment processors that are PCI-DSS compliant for all transactions.

Access Controls

Limit access to donor data on a need-to-know basis. Implement role-based permissions and regularly audit who has access to sensitive information.

Secure Storage

Store donor records in encrypted databases with automatic backup systems. Never save credit card information unless absolutely necessary and legally compliant.

Regular Updates

Keep donor management software current with latest security patches. Schedule quarterly reviews of data retention policies and purge outdated records safely.

CHAPTER 3

Volunteer Information Security

Volunteers are essential to nonprofit operations, but their personal information and access credentials require careful protection. Many volunteers use personal devices and may not be familiar with cybersecurity best practices.

01

Background Check Protection

Secure storage of screening documents with limited access and automatic expiration dates

02

Training Requirements

Mandatory security awareness training before granting system access to volunteers

03

Device Guidelines

Clear policies for personal device usage and secure remote access protocols

04

Offboarding Process

Immediate access revocation and data return procedures when volunteers transition out

Budget Tip: Free tools like Google Workspace for Nonprofits and Microsoft 365 Nonprofit offers include built-in security features perfect for managing volunteer access.

CHAPTER 4

Financial Data Safeguards

Banking Security

Enable multi-factor authentication on all financial accounts. Use dedicated computers for banking transactions and never access accounts on public WiFi.

Segregation of Duties

Separate financial responsibilities among multiple staff members. Require dual authorization for transactions over specified thresholds.

Regular Reconciliation

Conduct weekly bank reconciliations and monthly financial reviews. Set up automatic alerts for unusual account activity or large transactions.

Financial data breaches can be devastating for nonprofits, affecting both operational capabilities and donor confidence. Implement multiple layers of protection and maintain detailed audit trails for all financial activities.

CHAPTER 5

Grant and Reporting Data Protection

Secure Your Mission-Critical Documents

Grant applications and reports contain sensitive organizational data, financial projections, and strategic plans. Protecting this information prevents competitive disadvantages and maintains funder relationships.

→ **Version Control**

Use cloud-based collaboration tools with automatic versioning to prevent document conflicts and data loss

→ **Backup Strategy**

Maintain multiple backup copies of all grant documents with both cloud and offline storage options

→ **Sharing Protocols**

Use secure file transfer methods and password-protected documents when submitting sensitive grant materials

CHAPTER 6

Email and Communication Security

Email remains the primary attack vector for cybercriminals targeting nonprofits. Implementing strong email security practices protects your organization from phishing attacks, malware, and data breaches.

1

Phishing Awareness

Train all staff to recognize suspicious emails, verify sender addresses, and never click unknown links or attachments. Report suspected phishing attempts immediately.

2

Email Encryption

Use encrypted email services for sensitive communications. Enable TLS encryption for all email transmission and consider end-to-end encryption for highly confidential matters.

3

Spam Filtering

Implement robust spam filters and keep them updated. Regularly review quarantined messages and adjust filter settings to minimize false positives.

4

Mobile Security

Secure all mobile devices accessing organizational email with strong passwords, automatic locking, and remote wipe capabilities if devices are lost or stolen.

CHAPTER 7

Cloud Storage Best Practices

Choose Reputable Providers

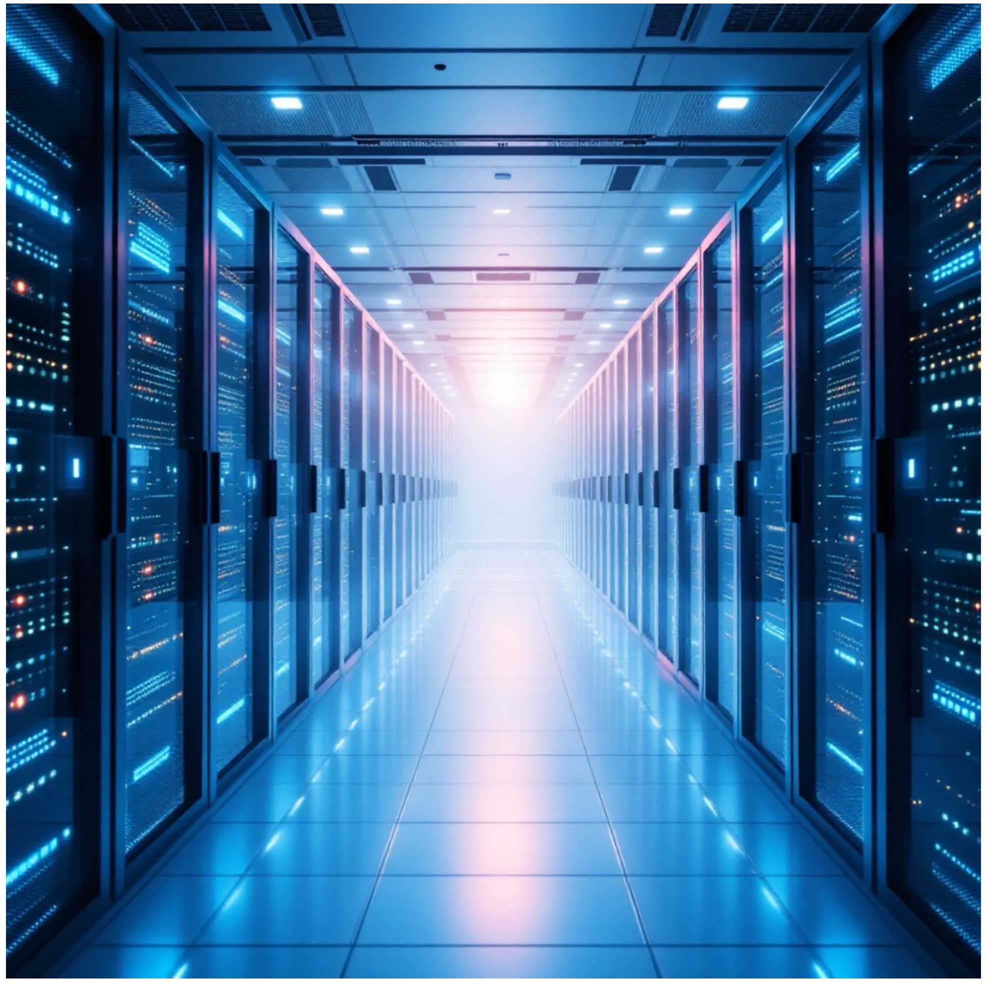
Select cloud services with strong security certifications, nonprofit pricing, and compliance with data protection regulations.

Enable All Security Features

Activate two-factor authentication, encryption at rest, and audit logging for all cloud storage accounts.

Organize and Control

Create clear folder structures with appropriate sharing permissions and regularly review access rights.



Cloud storage offers nonprofits affordable, scalable solutions for data management. However, proper configuration and ongoing management are essential to maintain security. Take advantage of nonprofit discounts from major providers while ensuring all security features are properly enabled.

CHAPTER 8

Board and Leadership Access

Board members and senior leadership often need remote access to sensitive organizational data, creating unique security challenges. Balancing accessibility with security is crucial for effective governance.

1 **Onboarding**

Provide security training and establish secure access credentials during board member orientation

2 **Ongoing Access**

Use secure board portals for document sharing and implement session timeouts for sensitive systems

3 **Device Security**

Require strong passwords and device encryption on personal devices accessing board materials

4 **Offboarding**

Promptly revoke access and retrieve organizational data when board terms conclude

Recommended: Consider using dedicated board management platforms like BoardEffect or Diligent Boards, which offer nonprofit pricing and built-in security features designed specifically for governance needs.

CHAPTER 9

Incident Response Basics

Be Prepared Before Incidents Occur

Every nonprofit needs a basic incident response plan, regardless of size or budget. Quick, coordinated action minimizes damage and speeds recovery.

Detection

Identify and verify the security incident immediately. Document all initial observations.

Containment

Isolate affected systems to prevent spread. Preserve evidence for investigation.

Recovery

Restore systems from clean backups. Verify security before resuming operations.

Review

Analyze the incident and update security measures to prevent recurrence.

CHAPTER 10

Compliance Requirements

Nonprofits must navigate various data protection regulations depending on their activities, location, and the types of data they collect. Understanding and meeting these requirements protects both your organization and the people you serve.

Privacy Policies

Maintain clear, accessible privacy policies that explain how you collect, use, store, and protect personal data. Update policies annually and whenever practices change.

Regulatory Standards

Identify which regulations apply to your nonprofit, such as GDPR for European donors, state privacy laws, or industry-specific requirements. Document compliance efforts.

Consent Management

Obtain and document explicit consent for data collection and use. Provide easy opt-out mechanisms and honor data deletion requests promptly.

Regular Audits

Conduct annual security and compliance audits. Address findings promptly and maintain documentation for funders and regulatory reviews.

Implementation Checklist

Your Action Plan

Start strengthening your nonprofit's data protection today with these prioritized steps. Focus on quick wins first, then build toward comprehensive security.

Immediate Actions (This Week)

- Enable multi-factor authentication on all accounts
- Update all software and operating systems
- Change weak or shared passwords
- Back up critical data to secure locations

Short-term Goals (This Month)

- Conduct security awareness training for staff
- Review and update access permissions
- Document your incident response plan
- Audit third-party service providers

Ongoing Commitments

- Monthly security training sessions
- Quarterly access reviews
- Annual policy updates
- Regular backup testing

About CSNP

Making cybersecurity knowledge accessible to everyone through education, community, and practical resources.

Our Programs

Business & Non-Profit Security • Family Cybersecurity • Kids Safety • Senior Digital Safety • Women's Security • Parents & Educators

Everything we offer is free

Visit csnp.org   Free Resources