Non - Profit Sector

TOP 10 Mandates for Organizational Safety

01

Enforce Strong, Unique Passwords

Avoid predictable passwords like "Nonprofit123!" Use long, complex passwords for email, CRM, and cloud platforms.

02

Activate Multi-Factor Authentication on All Accounts

Add an indispensable layer of protection for donor, accounting, and email systems.

03

Verify Donation and Volunteer Links Before Clicking

Scrutinize all donation-related emails. Confirm sender legitimacy; never click suspicious links.

04

Use Only Organization-Approved Tools

Employ your nonprofit's authorized CRM, file storage, and email platforms—avoid personal accounts or drives.

05

Protect Donor and Beneficiary Information

Never store or share sensitive information in unsecured documents or via unencrypted email; avoid public discussions.

06

Report Lost Devices Immediately

Notify IT or supervisors instantly if devices go missing, regardless of ownership.

07

Prohibit Sharing Login Credentials

Every user must maintain their own login; shared credentials compromise audits and security.

08

Keep Software Current

Apply updates promptly; security improvements are critical.

09

Limit Access to Necessary Data Only

Grant volunteers and interns minimal essential access, safeguarding the full donor database.

10

When Unsure, Consult Security Experts

If uncertain about any link or file, always check with IT or supervisors before proceeding.

vyings

Contact **VYINGS** for
fractional cybersecurity leadership.

www.vyings.com
info@vyings.com

Need help securing your organization?