ZENOPS PRACTICAL GUIDE

A NONPROFIT'S GUIDE TO

MFA

MULTIFACTOR AUTHENTICATION

A practical field guide for protecting people, data, and mission-critical systems

PEOPLE • DATA • MISSION

Matthew Bowley
CEO, Zenops, Inc.

2026 Edition

ABOUT THIS GUIDE

How to use this book

This guide is written for nonprofit executives, operations leaders, finance teams, board members, volunteers, and anyone responsible for keeping an organization safe with limited time and budget. It explains MFA in plain language and then turns the idea into a rollout plan you can use.

You do not need to read every page before taking action. If you need a fast start, read the first chapter, complete the account inventory in Chapter 3, and begin the 30-day plan in Chapter 8. If you are responsible for policy or oversight, pay special attention to the recovery, board, and governance sections.

IMPORTANT MFA is a security control, not a complete security program. Keep backups, patching, access reviews, phishing awareness, and incident response in place as well.

A note on scope

This field guide provides general educational information. It is not legal advice, compliance advice, or a substitute for a risk assessment. Your nonprofit may have additional obligations based on the information it handles, its funders, its contracts, its location, and the services it provides.

Contents

Chapter 1 Why MFA Matters to Nonprofits 3

Chapter 2 MFA in Plain English 5

Chapter 3 Find Your Digital Front Door 7

Chapter 4 Choose the Right MFA for the Risk 9

Chapter 5 Roll Out MFA Without Losing Trust 11

Chapter 6 Protect High-Risk People and Accounts 13

Chapter 7 Make MFA Part of Everyday Operations 15

Chapter 8 A 30-Day MFA Action Plan 17

Chapter 9 When Something Goes Wrong 19

Appendix A Sample MFA Policy 21

Appendix B Implementation Checklists 23

Appendix C Glossary 24

Appendix D Resources and Sources 25

CHAPTER 1

Why MFA Matters to Nonprofits

Your mission depends on more than good intentions. It depends on trusted access.

Nonprofits are often built around trust. Donors trust that their gifts will be used well. Clients trust that their information will be handled carefully. Employees and volunteers trust that the organization will provide the tools they need to do meaningful work. That trust now includes digital trust: the expectation that email, files, payments, records, and online services are protected.

A password alone is a weak foundation for that trust. Passwords are reused, shared, guessed, phished, and exposed in unrelated data breaches. Even a careful employee can be fooled by a convincing message or have a password stolen by malware. MFA adds a second checkpoint so that a stolen password is less likely to become a stolen account.

KEY TAKEAWAY The most important MFA decision is not which app to use. It is deciding that important accounts must have more than a password.

What can be lost when one account is compromised?

The damage from a compromised account is not limited to the account owner. Attackers look for the next useful step: a finance employee who can change payment instructions, a development employee who can access donor records, an executive whose email can authorize a transfer, or an administrator who can create new accounts and disable security controls.

1. Confidential donor, client, employee, or volunteer information
2. Access to banking, payroll, accounting, or grant-management systems
3. Cloud files containing contracts, case records, financial statements, or program data
4. The ability to send convincing messages from a trusted account
5. Social media, website, or fundraising accounts that represent the organization publicly
6. The organization's reputation and the confidence of the people it serves

MFA is a practical control for a practical problem

Cybersecurity can feel expensive and technical. MFA is different. Most major email, cloud, financial, donor, and collaboration platforms already support it. Many offer it at no additional cost or include it in

plans nonprofits already use. The work is primarily planning, configuration, communication, and follow-through.

That does not make MFA effortless. People may lose phones, change jobs, forget how to respond to an approval prompt, or worry that the process will slow them down. A good rollout treats those issues as design problems to solve, not reasons to leave accounts exposed.

A useful mindset

Do not think of MFA as something the IT department is imposing on everyone else. Think of it as a shared protection for the mission. The finance team protects the organization's money. The development team protects relationships with donors. Program staff protect the people they serve. MFA helps every team protect the access they depend on.

Before you move on

Take five minutes to discuss these questions with your leadership or technology team:

7. Which account would create the most damage if it were compromised today?
8. Which system would be hardest to recover if access were lost?
9. Who has the authority to protect or reset those accounts?

CHAPTER 2

MFA in Plain English

The technology is simple: prove you are the right person using more than one kind of evidence.

Multifactor authentication asks for two or more different types of proof before allowing access. The proof should come from separate categories. A password and the answer to another personal question are both things you know, so they are not as strong as using a password plus a device or biometric.

Factor	What it means	Examples
Something you know	A secret you can remember	Password, PIN
Something you have	A device or physical item you control	Authenticator app, security key, passkey
Something you are	A characteristic of you	Fingerprint, face recognition

Authentication is not the same as authorization

Authentication answers, "Who are you?" Authorization answers, "What are you allowed to do?" MFA improves authentication, but it does not automatically limit a user's permissions. A volunteer may successfully use MFA and still have too much access to a shared drive. Good security uses both strong sign-in and appropriate permissions.

Common MFA methods

The following methods are common in nonprofit environments. They are not equally resistant to phishing, and the best choice may differ by platform and user group.

10. Authenticator apps generate or approve sign-ins on a trusted mobile device. They are usually a strong, practical starting point.
11. Push notifications ask a user to approve a sign-in. They are convenient, but users must never approve an unexpected request.
12. Text-message codes are widely supported and better than password-only access, but phone numbers can be targeted through fraud or account takeover.
13. Security keys are physical devices that use cryptography to verify a sign-in. They are especially useful for administrators and other high-risk users.
14. Passkeys use cryptographic credentials stored on a device or security key and are designed to resist phishing. They may use a PIN or biometric to unlock the device.

15. Biometrics can make sign-in easy, but they are typically part of unlocking a device or passkey, not a replacement for every other control.

PRACTICAL RULE If phishing-resistant MFA is available, use it for administrators and high-value accounts. If it is not available, use the strongest supported method and keep moving.

What MFA does not do

16. It does not prevent every phishing attack.
17. It does not fix excessive permissions.
18. It does not replace backups, endpoint protection, patching, or email filtering.
19. It does not protect an account if users approve fraudulent prompts or share verification codes.
20. It does not eliminate the need to remove access when a person leaves.

MFA is powerful because it reduces the chance that a stolen password is enough. It becomes much stronger when combined with good account hygiene and an organization-wide habit of pausing before approving unexpected sign-ins.

CHAPTER 3

Find Your Digital Front Door

Before you turn on MFA, identify the accounts that matter most.

Many organizations begin with the system everyone remembers: email. Email is a smart first step, but it is not the whole picture. A nonprofit may have dozens of cloud services, old administrative accounts, shared logins, and contractor access that no one has reviewed recently.

The goal of an account inventory is not to create a perfect database on day one. The goal is to see enough of the environment to make good decisions. Start with systems that can expose sensitive information, move money, change the public voice of the organization, or create more accounts.

Build a simple system inventory

For each system, capture the owner, purpose, users, administrator, sensitivity, MFA status, and recovery method. A spreadsheet is sufficient for a small nonprofit. A password manager or governance platform may be better as the program grows.

System group	Examples	First question
Identity and email	Microsoft 365, Google Workspace, email hosting	Can an attacker reset other accounts from here?
Money	Banking, accounting, payroll, payment processors	Can this account change or approve a payment?
People and relationships	CRM, donor platform, case-management system	What personal or donor information is stored here?
Files and collaboration	OneDrive, SharePoint, Google Drive, Dropbox	Which folders contain sensitive or irreplaceable data?
Public presence	Website, social media, fundraising pages	Could this account damage trust if hijacked?
Technology administration	RMM, VPN, domain registrar, backup console	Could this account disable security or recovery?

Rank accounts by impact

You do not need a complicated scoring system. Use three questions: What could happen if this account were stolen? How many other systems could it reach? How difficult would recovery be? The answers help you decide where to require the strongest MFA first.

21. Critical: administrator, banking, payroll, identity, backup, domain, or security accounts.

22. High: executive, finance, development, HR, donor, case-management, and grant-management accounts.
23. Standard: other employee, volunteer, and contractor accounts that still access organizational data.
24. Review: shared, inactive, legacy, service, and emergency accounts that may not have a clear owner.

DO NOT FORGET A shared account is not a security strategy. Where possible, give each person an individual login, require MFA, and use delegated access or role-based permissions.

Look for hidden access

The most dangerous account may not be the one used every day. Check old employees, former volunteers, contractors, board members, temporary staff, personal email addresses used for administration, application owners, and accounts created during a crisis that were never cleaned up.

Also check recovery addresses and phone numbers. If a former employee's personal email or an unknown phone number can reset an administrator account, MFA is not the end of the risk. Recovery information is part of the security boundary.

CHAPTER 4

Choose the Right MFA for the Risk

Use the strongest practical method for the people and systems that matter most.

There is no single MFA method that fits every person, device, and application. A nonprofit may need to support staff who work in an office, field workers who share devices, volunteers who use personal phones, and administrators who need a higher level of protection.

The right approach is to set a minimum standard and then use stronger methods where the risk is higher. This avoids two common mistakes: choosing the weakest method for everyone, or creating a complex program that people cannot use consistently.

A practical method hierarchy

Method	Use it when	Watch for
Passkeys or security keys	Administrators, executives, finance, identity, backup, and other high-value accounts	Spare key storage, enrollment, loss and replacement process
Authenticator app	Most employees and volunteers with a supported phone or device	Device changes, lost phones, backup enrollment
Push approval	Users need a simple approval workflow and understand prompt safety	MFA fatigue and accidental approvals
Text-message code	A platform offers no stronger option or a user needs a transition path	Number takeover, shared phones, delayed messages
Email code	Temporary or low-risk access where no better option exists	Email compromise can defeat the second step

Phishing-resistant MFA

Phishing-resistant MFA uses cryptographic proof tied to the legitimate website or application. The user does not type a code into a fake page that an attacker can capture. Security keys and passkeys are common examples. These options are worth prioritizing for accounts that can move money, administer identity, access backups, or expose large amounts of personal information.

DECISION Do not delay the entire MFA rollout while you evaluate the perfect technology. Establish a baseline now, then raise the standard for high-risk accounts as you are ready.

Design for real people

25. Some users cannot use a personal phone for work. Offer an approved alternative such as a security key or managed device.
26. Some staff work in locations with limited cellular service. Do not rely only on SMS or push notifications.
27. Some volunteers participate only a few times each year. Document a simple enrollment and recovery process.
28. Some teams share front-desk or program devices. Use individual accounts and device policies where possible.
29. Some users need accessibility accommodations. Confirm that the MFA method works with assistive technology and does not create avoidable barriers.

Security that people cannot use becomes security that people work around. Inclusion and usability are part of the design, not optional extras.

CHAPTER 5

Roll Out MFA Without Losing Trust

A successful rollout is a change-management project as much as a technical project.

People resist security changes when the reason is unclear, the timing is poor, or the support is missing. The fix is not to avoid the control. The fix is to communicate early, pilot with a small group, and provide a reliable path when something goes wrong.

Before the rollout

30. Name an executive sponsor who can explain why MFA supports the mission.
31. Choose an owner who can make configuration decisions and coordinate support.
32. Confirm licensing and platform capabilities before announcing a deadline.
33. Create short instructions with screenshots or links to the vendor's current help pages.
34. Decide how users will recover from a lost phone, replacement device, or locked account.
35. Pilot with a small group that includes an administrator, a finance user, a field user, and someone less comfortable with technology.

Write the message in mission language

A good announcement should answer four questions: What is changing? Why is it changing? When must I complete it? Where do I get help? Keep the message direct and respectful. Avoid implying that someone who struggles with MFA is careless or uncooperative.

SAMPLE MESSAGE Starting on [date], we will add an extra sign-in step to protect our email and organizational accounts. This helps prevent someone who has stolen a password from accessing our systems. You will need your approved phone, authenticator app, or security key. If you need help, contact [support contact] before the deadline.

A simple rollout sequence

36. Configure policies and test them with pilot users.
37. Enroll administrators and high-risk accounts first.
38. Send the announcement and enrollment instructions.
39. Hold short enrollment sessions or office hours.
40. Monitor sign-ins, failed enrollment, lockouts, and support requests.

41. Follow up with people who have not enrolled.
42. Enforce MFA after the support window, with a documented exception process.
43. Review the results and improve the process before the next group.

Avoid permanent exceptions

Exceptions may be necessary. A shared medical device, a service account, a legacy application, or a user with a documented accessibility need may require a different control. Every exception should have an owner, a reason, a compensating control, and a review date. An exception with no expiration date tends to become the normal way of working.

CHAPTER 6

Protect High-Risk People and Accounts

The accounts with the most authority deserve the strongest protection and the most careful recovery process.

A nonprofit does not need to treat every account identically. Executives, finance staff, development leaders, IT administrators, and identity administrators often face greater risk because their accounts can approve payments, disclose information, or change the security of the entire environment.

High-risk users

44. Executive leadership and anyone whose name could be used to authorize a payment or sensitive action
45. Finance, payroll, accounts payable, and anyone who manages bank or payment access
46. Development and fundraising staff with donor or campaign systems
47. HR staff with employee records
48. IT, identity, backup, domain, website, and security administrators
49. Board members or volunteers with access to financial, donor, or executive information

Use separate administrator accounts

An administrator should have a standard daily account and a separate administrator account used only for administrative tasks. This reduces the chance that a routine email or web session exposes powerful privileges. Both accounts need MFA, and administrator accounts should use a stronger method whenever the platform supports it.

Protect the recovery path

Recovery is where many otherwise strong systems become weak. Decide how a user proves identity when a phone is lost, a security key breaks, or an account is locked. Do not reset MFA based only on an email request that could come from a compromised mailbox.

50. Use a documented identity-verification process for resets.
51. Require a second approved person for administrator recovery when practical.
52. Store backup codes or spare security keys in a controlled location.
53. Review recovery email addresses and phone numbers regularly.
54. Record when a recovery action occurs and who approved it.

HIGH-RISK RULE The person who can reset MFA should not be protected only by the same email account whose MFA is being reset.

Emergency accounts

Some organizations maintain one or more emergency or break-glass accounts for a major outage. These accounts should be rare, documented, monitored, and protected with strong credentials. Store the recovery information securely, limit who can use it, and test the process on a schedule. An emergency account that nobody can find is not useful; an emergency account that is used every day is not an emergency account.

CHAPTER 7

Make MFA Part of Everyday Operations

MFA works best when it becomes routine instead of a one-time project.

Turning on MFA is a milestone, not the finish line. People join and leave. Devices change. New applications are adopted. Vendors change their sign-in methods. A nonprofit needs a small set of repeatable operational habits to keep MFA working.

Onboarding

MFA enrollment belongs in the onboarding checklist, before a new employee receives access to sensitive systems. The manager should confirm the role and required systems. The technology owner should provision the account, enforce MFA, and verify that recovery information is correct. The user should understand how to report a suspicious prompt or lost device.

Offboarding

When a person leaves, disable the account promptly, revoke sessions and tokens where possible, remove group membership, transfer needed files, and review delegated access. This includes volunteers, contractors, interns, temporary workers, and board members whose terms have ended.

Quarterly access review

At least quarterly, review administrator accounts, inactive accounts, shared accounts, MFA registration, recovery methods, and exceptions. The review does not need to be complicated. It needs to have a named owner and evidence that the questions were answered.

Review question	What good looks like
Who can administer identity or email?	Every account has a current owner, strong MFA, and only the permissions needed.
Who can move or approve money?	Financial access is limited, individually assigned, and protected by MFA.
Which accounts are inactive?	Inactive accounts are disabled or have a documented business reason.
Can users recover their own accounts safely?	Recovery methods are current and reset procedures are documented.
Which exceptions remain?	Every exception has a reason, owner, compensating control, and review date.

Watch for suspicious sign-in behavior

55. Unexpected MFA prompts or repeated approval requests
56. Sign-ins from unfamiliar locations or devices
57. New forwarding rules or mailbox delegates
58. Password-reset messages the user did not request
59. Changes to banking, payment, donor, or website information
60. A user reporting that a file, message, or setting changed unexpectedly

MFA alerts are signals, not annoyances. A user who reports an unexpected prompt may be giving your organization its earliest warning that a password has been compromised.

CHAPTER 8

A 30-Day MFA Action Plan

A month is enough time to move from uncertainty to a working baseline.

The following plan is designed for a small or mid-sized nonprofit. Adjust the pace to your staffing, platform, and risk. The sequence matters more than the exact calendar. If you have a serious active incident, stop and use your incident-response process before beginning a broad rollout.

Timing	Focus	Deliverable
Days 1-5	Ownership and inventory	Sponsor, technical owner, system list, high-risk account list
Days 6-10	Policy and design	MFA standard, recovery process, exception process, user message
Days 11-15	Pilot	Pilot users enrolled, problems documented, instructions improved
Days 16-22	High-risk rollout	Administrators, finance, executives, and key systems protected
Days 23-28	Organization rollout	Employees and volunteers enrolled with support
Days 29-30	Enforcement and review	MFA enforced, exceptions recorded, next review scheduled

Days 1-5: establish ownership

61. Name the executive sponsor and technical owner.
62. List identity, email, finance, donor, file, website, social, backup, and remote-access systems.
63. Identify administrators, finance users, executives, development users, and other high-risk accounts.
64. Find inactive accounts, shared accounts, service accounts, and unknown recovery methods.

Days 6-10: decide the standard

65. Choose the minimum MFA method for standard users.
66. Choose stronger methods for administrators and high-risk accounts.
67. Document enrollment, device replacement, lost-device, and emergency recovery steps.
68. Draft the user announcement and support instructions.

Days 11-15: run the pilot

69. Enroll a small group representing different roles and work locations.
70. Test sign-in from normal devices and a new device.
71. Test a lost-device recovery scenario without creating a real outage.
72. Capture questions and rewrite instructions in plain language.

Days 16-28: enroll and support

Protect high-risk accounts first, then open enrollment to the broader organization. Use office hours, short demonstrations, and direct support. Monitor the platform for failures and watch for users who have not enrolled. If the same problem appears more than once, update the process instead of answering the same question forever.

Days 29-30: enforce and improve

Enforce MFA for accounts that should have it. Document approved exceptions. Review the first month of enrollment and support data. Schedule a quarterly access review and choose the next security improvement, such as stronger MFA for administrators, better backups, or a phishing-awareness exercise.

SUCCESS MEASURE The first success metric is not a perfect percentage. It is knowing which accounts are protected, which are not, why they are not, and who owns the next action.

CHAPTER 9

When Something Goes Wrong

Prepare for lost devices, suspicious prompts, and compromised accounts before they happen.

MFA reduces risk, but it does not eliminate mistakes or attacks. A user may approve a fraudulent prompt. A device may be stolen. A password may be exposed and an attacker may try to register a new authentication method. The quality of your response determines how much damage follows.

If a user receives an unexpected MFA prompt

73. Do not approve the request.
74. Capture the time and application if it is safe to do so.
75. Report the event to the designated support contact.
76. Change the password from a trusted device if instructed.
77. Review recent sign-ins, sessions, forwarding rules, and new authentication methods.

If a device is lost or stolen

78. Report the loss immediately. Do not wait to see whether the device turns up.
79. Revoke or block the device and its authentication session where possible.
80. Remove the lost authenticator and issue a replacement method.
81. Review the account for suspicious activity and reset credentials if needed.
82. Document the event and update the recovery process if the response was unclear.

If an account may be compromised

Treat the event as an incident, not only a password-reset request. Disable or restrict the account, revoke sessions, check mailbox rules and delegates, review activity, protect connected systems, and preserve information that may help determine what happened. Contact your IT provider, insurance carrier, legal counsel, or law enforcement partners as appropriate to your situation.

REMEMBER Speed matters, but panic creates mistakes. Follow a written process and record decisions as you go.

Learn from the event

After the account is secure, ask what allowed the problem to continue. Was the user unsure where to report it? Was the recovery path too easy to abuse? Did an application bypass the organization's MFA policy? Did a former user still have access? Every incident should improve the next version of your controls and instructions.

APPENDIX A

Sample MFA Policy

The following sample is a starting point. Adapt it to your organization, systems, contracts, and risk. Have the appropriate leadership or legal advisor review it before adoption.

Purpose

[Organization] requires multifactor authentication to reduce the risk of unauthorized access to organizational systems, information, funds, and services.

Scope

This policy applies to employees, volunteers, contractors, interns, board members, service providers, and other people who access [Organization] systems or information. It applies to organizational accounts, approved personal devices used for access, and systems connected to the organization's identity platform.

Requirements

83. MFA is required for email, identity, financial, donor, file-storage, remote-access, administrator, and other designated systems.
84. Users must use the approved MFA method and must not share passwords, verification codes, security keys, or approval requests.
85. Users must not approve an MFA prompt they did not initiate and must report unexpected prompts promptly.
86. Administrators and other high-risk accounts must use the strongest supported MFA method designated by [Organization].
87. Accounts must be reviewed and access must be removed when a person changes roles or leaves the organization.
88. MFA exceptions require documented approval, a business reason, a compensating control, an owner, and a review date.

Lost devices and recovery

Users must report a lost or stolen authentication device immediately to [contact]. MFA resets and recovery actions must follow the documented identity-verification process. Administrator recovery should require additional approval when practical.

Enforcement

Failure to follow this policy may result in restricted access, removal of access, or other action consistent with organizational policy. The policy owner will review this document at least annually and after a significant security incident or technology change.

APPENDIX B

Implementation Checklists

Leadership checklist

89. We have named an executive sponsor and an accountable operational owner.
90. We understand which systems hold sensitive information or control money.
91. We have set a deadline and a support plan that staff can realistically follow.
92. We have approved a recovery and exception process.
93. We review MFA status, administrator access, and exceptions on a regular schedule.

Technical checklist

94. MFA is enabled for identity and email.
95. Administrator accounts are individually assigned and protected with stronger MFA where possible.
96. Recovery email addresses, phone numbers, and backup methods are current.
97. Sessions, tokens, forwarding rules, delegates, and connected applications are reviewed after suspicious activity.
98. Joiner, mover, and leaver procedures include MFA enrollment and removal.
99. Exceptions are documented with owners, compensating controls, and review dates.

Staff checklist

100. I know how to enroll in the approved MFA method.
101. I know never to approve an unexpected MFA prompt.
102. I know where to report a suspicious prompt or lost device.
103. I do not share passwords, codes, security keys, or approval requests.
104. I know how to get help when I replace my phone or change devices.

APPENDIX C

Glossary

Authentication: The process of verifying who a person, device, or service is.

Authorization: The permissions granted after authentication, such as read, edit, approve, or administer.

Authenticator: A method or device used to prove identity, such as an app, security key, or passkey.

Break-glass account: A tightly controlled emergency account used when normal administrative access is unavailable.

MFA fatigue: A situation where repeated approval prompts cause a user to approve a request without checking it.

Passkey: A cryptographic sign-in credential designed to resist phishing and unlocked by a device PIN or biometric.

Phishing-resistant MFA: MFA that uses cryptographic proof tied to the legitimate service so a fake website cannot easily capture the sign-in.

Recovery method: A process or alternate authenticator used to regain access after a device is lost or an account is locked.

Security key: A physical device that uses cryptographic authentication, often through FIDO2 or WebAuthn.

Service account: An account used by an application or system rather than a person; it needs an owner and special controls.

Session or token: A temporary credential that keeps a user signed in after authentication.

APPENDIX D

Resources and Sources

The recommendations in this guide are informed by the following public resources. Technology and guidance change, so check the source pages for current details before adopting a specific configuration.

CISA: Require Multifactor Authentication. Practical guidance for small and medium-sized organizations. https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/require-strong-passwords

CISA: Mitigating Cyber Threats with Limited Resources. Joint guidance for civil society organizations, including phishing-resistant MFA recommendations. https://www.cisa.gov/sites/default/files/2024-05/joint-guide-mitigating-cyber-threats-with-limited-resources-guidance-for-civil-society-508c_3.pdf

NIST SP 800-63B: Digital Identity Guidelines. Current guidance on authentication processes and authenticators. https://pages.nist.gov/800-63-4/sp800-63b.html

CISA: Recognize and Report Phishing. Plain-language guidance for recognizing phishing and using MFA. https://www.cisa.gov/secure-our-world/recognize-and-report-phishing

TechSoup: Cybersecurity Basics Your Nonprofit Needs to Know. Nonprofit-focused cybersecurity fundamentals and awareness ideas. https://blog.techsoup.org/en-us/posts/cybersecurity-basics-your-nonprofit-needs-to-know

NEXT STEP Choose one high-value system, one accountable owner, and one date. Start there.