Place Organization Name Here

MFA Roll-Out Checklist

MULTI-FACTOR AUTHENTICATION (MFA) ROLLOUT CHECKLIST

A Center4 Cybersecurity Implementation Guide for Nonprofits

PURPOSE

This checklist helps nonprofit organizations implement Multi-Factor Authentication (MFA) across their systems to reduce the risk of phishing, ransomware, and account compromise.

MFA is often required for:

- Cybersecurity grants
- Federal funding programs
- Cyber insurance eligibility
- Compliance frameworks (HIPAA, PCI, etc.)

PHASE 1: PLANNING & ASSESSMENT

Identify Systems Requiring MFA

- ☐ Email system (Microsoft 365 / Google Workspace)
- ☐ Financial systems
- ☐ Donor database / CRM
- ☐ Payroll system
- ☐ Cloud storage platforms
- ☐ Remote desktop access
- ☐ VPN access
- ☐ Administrator accounts
- ☐ VoIP admin portals
- ☐ Website hosting control panel

---

inventory users

- ☐ Create list of all active users
- ☐ Identify privileged/administrator accounts
- ☐ Identify shared or legacy accounts
- ☐ Remove terminated users
- ☐ Remove unnecessary access

---

choose mfa method

Select primary MFA method:

- ☐ Authenticator app (Recommended – Microsoft Authenticator, Google Authenticator)
- ☐ Hardware security key
- ☐ Push notification
- ☐ SMS (least preferred but acceptable short-term)

Document chosen standard:

PHASE 2: POLICY DEVELOPMENT

- ☐ Update Cybersecurity Policy to require MFA
- ☐ Notify staff of upcoming rollout
- ☐ Set enforcement deadline
- ☐ Provide clear instructions to users
- ☐ Establish support contact

Sample Policy Statement:

"All staff must use multi-factor authentication for access to organizational systems. MFA must be enabled on all cloud platforms, financial systems, and administrative accounts."

PHASE 3: PILOT DEPLOYMENT

- ☐ Test MFA with IT team first
- ☐ Test with Executive Director and finance team
- ☐ Validate login experience
- ☐ Confirm no workflow disruptions
- ☐ Document common issues

Pilot Start Date:

Pilot End Date:

PHASE 4: ORGANIZATION-WIDE DEPLOYMENT

Communication Plan

- ☐ Send advance notice email
- ☐ Provide FAQ document
- ☐ Offer short training session
- ☐ Provide step-by-step setup guide

---

deployment steps

- ☐ Enable MFA enforcement in admin portal
- ☐ Require registration upon next login
- ☐ Confirm backup authentication method
- ☐ Confirm recovery email and phone number
- ☐ Verify administrator accounts secured first

PHASE 5: SPECIAL CONSIDERATIONS

Board Members

- ☐ Ensure Board email accounts have MFA
- ☐ Provide simplified instructions

Volunteers

- ☐ Determine whether MFA required based on access
- ☐ Disable unnecessary access

Shared Devices

- ☐ Ensure individual user accounts used
- ☐ Remove shared credentials

PHASE 6: BACKUP & RECOVERY PLANNING

- ☐ Ensure IT admin has break-glass emergency account
- ☐ Secure backup authentication codes
- ☐ Store emergency recovery instructions securely
- ☐ Document account recovery process

Emergency Contact:

PHASE 7: MONITORING & ENFORCEMENT

- ☐ Review MFA compliance report monthly
- ☐ Disable accounts without MFA
- ☐ Review failed login attempts
- ☐ Audit privileged accounts quarterly

PHASE 8: RISK REDUCTION VALIDATION

After deployment, confirm:

- ☐ MFA enabled for 100% of users
- ☐ MFA enabled for 100% of admins
- ☐ No SMS-only configurations (unless unavoidable)
- ☐ Legacy authentication disabled
- ☐ Conditional access policies configured (if available)

PHASE 9: DOCUMENTATION FOR GRANTS & INSURANCE

Maintain documentation of:

- ☐ Date MFA implemented
- ☐ Systems covered
- ☐ Percentage of user compliance
- ☐ Screenshots of enforcement settings
- ☐ Updated security policy

This documentation may be required for:

- Cybersecurity grant applications
- Cyber insurance underwriting
- Federal program compliance

POST-IMPLEMENTATION REVIEW

Date Completed: _____

Number of Users Protected: _____

Remaining Gaps:

_____

_____

_____

Next Review Date: _____

---

about this checklist

Multi-Factor Authentication is one of the highest-impact, lowest-cost cybersecurity controls available to nonprofits.

This checklist was created by Center4 to help organizations protect their staff, donors, and communities while strengthening eligibility for funding programs and cyber insurance.

For additional cybersecurity resources, visit:

- https://www.center4.com
- https://www.allsector.com