CYBERSECURITY FIELD GUIDE

FOR SMALL BUSINESSES AND NONPROFITS

Updated on
12/20/2025

WHAT'S INSIDE	● Five practical steps to protect your organization’s information ● Actionable items that you can perform at your convenience

About this Guide

This free guide was created by **Fall River Data Security Solutions** to help small businesses and nonprofits take practical, achievable steps to better protect their information, systems, and people.

Cybersecurity does not have to be overwhelming or highly technical. The goal of this kit is to provide clear guidance you can act on immediately, regardless of your organization’s size or budget. There are no sales pitches here—only proven practices that reduce real-world risk.

How to Use This Kit

- You do **not** need to do everything at once.
- Start with the sections that address your biggest risks.
- Assign ownership for each task so progress doesn’t stall.
- Revisit this guide periodically as your organization grows.

Each section includes:

- Why the control matters
- Practical steps to implement it
- A short checklist you can use internally

1. Use a Password Manager

Why This Matters

Password reuse is one of the most common causes of security incidents. When a single password is compromised, attackers often gain access to multiple systems, email accounts, and cloud services. This can lead to data theft, financial loss, and operational disruption.

Password managers reduce this risk by generating and storing long, unique passwords for every account in a secure, encrypted vault.

Practical Implementation Steps

- Select a reputable password manager that supports teams or businesses.
- Require unique passwords for every system and service.
- Start rollout with leadership, finance, IT administrators, and anyone with access to sensitive data.

- Provide a short walkthrough or written guide so staff know how to use the tool.
- Require all new accounts to be stored in the password manager.

Commonly Used Password Managers

- **NordPass** – Includes data breach scanning and email masking
- **1Password** – Supports passwords, passkeys, and secure notes
- **Proton Pass** – Generous free tier and open source
- **Dashlane** – Widely trusted in enterprise environments

ACTIONABLE STEPS	STATUS
Password manager selected	□
Leadership accounts onboarded	□
Financial and email admin accounts secured	□
Staff guidance distributed	□
Policy requiring password manager use established	□

2. Create and Maintain Backups

Why This Matters

Backups are your last line of defense against ransomware, accidental deletion, hardware failure, and natural disasters. Without reliable backups, recovery can be slow, costly, or impossible.

Practical Implementation Steps

- Identify critical data (financial records, HR files, donor/customer lists, contracts).
- Maintain at least two backups:
    - One cloud-based
    - One offline or isolated from your main network
- Automate backups where possible.
- Periodically test backups by restoring files.

Common Backup Options

- **Backblaze** – Automated backups with flexible rules
- **Sync** – Secure cloud storage with long-term vault options
- **Google Workspace (Drive)** – Collaboration-friendly with generous free tier
- **Microsoft OneDrive / Microsoft 365** – Deep integration with Office tools

ACTIONABLE STEPS	STATUS
Critical data identified	□
Cloud backup configured	□
Offline or isolated backup configured	□
Backups automated	□
Restore test completed	□

3. Patch and Update Software

Why This Matters

Attackers routinely exploit known vulnerabilities in outdated software. Many successful attacks occur not because of advanced techniques, but because systems were never updated.

Practical Implementation Steps

- Enable automatic updates on operating systems and common applications.
- Assign responsibility for monitoring updates to a specific role.
- Maintain a simple list of critical systems and software.
- Schedule updates during low-impact times.
- Use a test or “sandbox” environment if updates have historically caused issues.

ACTIONABLE STEPS	STATUS
Automatic updates enabled	□
Update owner assigned	□
Software inventory maintained	□
Update schedule documented	□

4. Stay Informed with Cybersecurity Newsletters

Why This Matters

Cyber threats evolve quickly, but staying informed does not require deep technical expertise. A small amount of regular awareness helps organizations avoid emerging scams and respond faster to new risks.

Practical Implementation Steps

- Subscribe to 1–3 trusted cybersecurity newsletters.
- Choose sources that focus on small organizations and plain-language summaries.
- Assign a “security champion” to review and share highlights.
- Share one practical tip per month with staff.

ACTIONABLE STEPS	STATUS
Newsletters selected	□
Security champion assigned	□
Monthly sharing process defined	□
Monthly sharing process defined	□

5. Implement Basic Security Policies

Why This Matters

Written policies reduce uncertainty and help staff make safer decisions under pressure. They turn expectations into repeatable behavior and reduce reliance on individual judgment.

Key Policies to Start With

Acceptable Use Policy

Defines how staff may use:

- Email and internet access
- Organization-owned devices
- Public Wi-Fi and remote access
- External storage and downloads

Information Security Standard

Documents the expectations for:

- Data storage and handling
- Access controls
- Device security
- Record retention

Incident Response Procedure

Outlines:

- How to recognize a potential incident
- Who is in charge during an incident
- Who must be notified
- Immediate response steps
- Recovery and follow-up actions

Practical Implementation Steps

- Keep policies short and readable.
- Use clear, non-technical language.
- Review policies briefly in a team meeting.
- Have staff acknowledge they've read them.

ACTIONABLE STEPS	STATUS
Acceptable use policy drafted	□
Information security standard documented	□
Incident response procedure written	□
Staff acknowledgment collected	□

Final Thoughts

Improving information security is a long-term effort, not a one-time project. The steps in this guide address the most common and impactful risks facing small organizations today.

You do not need perfect security to significantly reduce risk—you need consistent, intentional practices. Starting with these five areas will put your organization on a much stronger footing and make future improvements easier to manage.