J3 Systems Group Quick Resource

IT Best Practices Guide

A simple guide for keeping a small business IT environment organized and secure.

Practical guidance for small businesses and nonprofit organizations

Prepared by J3 Systems Group LLC

Overview

Strong IT habits do not need to be complicated. This guide gives business owners a practical starting point for keeping users, devices, files, and vendor access under control.

Who This Is For

- Small business owners without a full internal IT department.
- Office managers who coordinate users, devices, and vendors.
- Nonprofit teams that need simple operating standards.

Best Practice Areas

Password safety

- Use long unique passwords for every business account.
- Avoid saving passwords in shared documents, spreadsheets, or browser profiles used by multiple people.
- Use a trusted password manager to keep access organized.

MFA

- Turn on MFA for email, file storage, financial systems, payroll, and administrator accounts.
- Use app based approval or security keys when available.
- Review backup methods before an employee leaves.

Backups

- Know what systems are backed up and how often backups run.
- Test recovery before a real emergency.
- Keep backup ownership documented.

Software updates

- Keep Windows, macOS, browsers, Microsoft 365 apps, and security tools current.
- Schedule updates so they do not depend on memory.
- Track devices that are too old to support current updates.

Device tracking

- Maintain a list of company laptops, desktops, phones, and tablets.
- Record assigned user, serial number, purchase date, and condition.
- Collect devices during employee offboarding.

Email security

- Train staff to report suspicious messages.
- Review forwarding rules and mailbox access.
- Use spam, phishing, and malware protection settings.

File sharing

- Use business controlled storage instead of personal drives.
- Review external sharing regularly.
- Name shared folders clearly so permissions are easier to understand.

Vendor access

- Document vendors who can access systems or data.
- Remove access when projects end.
- Avoid shared vendor accounts whenever possible.

Documentation

- Document onboarding, offboarding, password reset, purchasing, and support processes.
- Store documentation where leadership can find it.
- Review documents after major changes.

When Outside Help Makes Sense

Ask for help when admin roles are unclear, business data is spread across personal accounts, access removal depends on memory, security alerts are not being reviewed, or the organization is not sure which settings are currently protecting users and files.

Quick Review

☐ User access is reviewed monthly.
☐ Devices are tracked.
☐ Backups are tested.
☐ Vendor access is documented.
☐ Offboarding steps are repeatable.

Conclusion

Consistent IT practices help reduce emergencies, protect company data, and make daily operations easier to manage.

Need help reviewing your Microsoft 365, Google Workspace, offboarding, or small business IT security setup?

J3 Systems Group LLC provides practical IT support, documentation, cloud administration, and security focused reviews for small businesses and nonprofit organizations.

Contact J3 Systems Group LLC to request a practical review and clear next steps.