



Secure Password Management Guide

A simple guide to stronger passwords, safer sharing, and secure access habits for employees and business owners.

Your IT Department. Your Cybersecurity Team. Your Technology Partner.

Network Solutionist, LLC

Serving Wilmington, Newark, Middletown, Dover, Rehoboth Beach, and businesses across Delaware.



Password Rules That Actually Help

- Use long, unique passwords or passphrases for every account.
- Never reuse business passwords on personal websites.
- Use a password manager approved by the business.
- Enable MFA for important accounts.
- Do not share passwords through email, text messages, chat, or spreadsheets.
- Remove access when employees, vendors, or contractors leave.
- Use separate accounts for admin work and everyday work.
- Review saved browser passwords and unmanaged credential storage.
- Change passwords immediately when compromise is suspected.
- Protect recovery email accounts and phone numbers.

Password Manager Rollout Checklist

Done	Security Item	Why It Matters
☐	Select a business password manager.	Centralized management improves visibility and control.
☐	Create shared vaults by department or function.	Shared access should be structured and approved.
☐	Require MFA for password manager access.	The password manager becomes a critical security system.
☐	Import and clean up existing credentials.	Remove duplicates, weak passwords, and outdated accounts.
☐	Train employees on secure sharing.	Users need to know how to share without exposing secrets.
☐	Set an offboarding process.	Departing users should lose access quickly.
☐	Review vault access regularly.	Access should match current job duties.

Red Flags

- Passwords stored in spreadsheets or notes.
- One shared login used by many employees.
- Former employees still know vendor or admin passwords.
- MFA recovery codes stored in the same place as passwords.
- Passwords sent to vendors or coworkers without expiration or tracking.



Helpful Reference Points

- FTC guidance states a strong password is at least 12 characters and recommends never reusing passwords or sharing them by phone, text, or email.
- CISA small business resources include password managers as a recommended security topic.

Disclaimer

This guide is for general educational purposes and does not replace a formal cybersecurity assessment, compliance review, or incident response engagement.

Need help turning this into an action plan?

Network Solutionist, LLC can help assess, secure, monitor, and support your business technology environment. (302) 485-9850 | info@nsolutionist.com | nsolutionist.com

