SOP F — Router & Printer Hardening (Quarterly)

ToroTek LLC — Standard Operating Procedure

Close the ‘factory default’ doors attackers love. Update firmware, kill WPS, and set strong admin passwords.

Before You Start

- Admin logins to router/modem and each networked printer/MFD.
- 30–60 minute maintenance window; warn the team about brief outages.
- Password manager ready to store/rotate new admin credentials.

Step-by-Step

1. **Step 1.** Router: sign in; change the admin username/password to a long unique password; save in the password manager.
2. **Step 2.** Update router firmware; enable WPA3 or WPA2-AES; disable WPS; set a unique SSID; create a Guest Wi-Fi.
3. **Step 3.** Printer/MFDs: sign in to web admin; change admin password; disable Wi-Fi Direct if unused; update firmware.
4. **Step 4.** Turn off remote admin or cloud print features not in use; set jobs not to store unless required.
5. **Step 5.** Document the final configuration and store screenshots in your records.

Done-Right Checklist

- All new admin credentials saved in the password manager.
- Office devices reconnect to Wi-Fi; guest network works as expected.
- Firmware versions recorded; WPS disabled; WPA3/WPA2-AES in use.
- Default passwords eliminated on all printers.

When to Call ToroTek

- Firmware update fails or device becomes unstable after changes.
- Can’t enable WPA2-AES/WPA3 (legacy hardware).
- Printers expose features your team relies on—need a safer configuration.

Pro Tips

- Rotate admin passwords quarterly or when staff with access leave.
- Segment guest Wi-Fi from staff network to isolate risky devices.

- Consider replacing legacy routers that can’t support WPA2-AES at minimum.

Need help? ToroTek is here.
Call/Text: 619-376-6995
Support: help@toro-tek.com
Web: torotekllc.com

Updated: 2025-08-13