Smith’s Construction LLC

Cybersecurity Disaster Recovery Plan (DRP)

Version 1.0 — Last Updated: [Insert Date]

1. Introduction

When it comes to cyberattacks, it is no longer a matter of “if”, but “when”. Small businesses face increasing exposure to cyber threats, and the impact of any incident depends on the strength of their cybersecurity posture. This DRP ensures Smith’s Construction LLC can respond, recover, and resume operations efficiently.

2. Scope

Systems in scope include all Windows desktops, network printers, on-site NAS devices, IoT devices, AWS backups, local network infrastructure, and cloud services. All employees, contractors, vendors, and remote workers fall under this policy.

3. Roles, Responsibilities & Communication

Key roles include the Incident Response Coordinator, IT Support, Data Owners, Executive Management, and all employees. Communication channels include company phones, personal mobiles, emergency email, and vendor contacts.

4. Critical Assets & Priority

Critical assets: business data, Windows desktops, network infrastructure, cloud services, printers, and IoT devices. Recovery priority begins with restoring network infrastructure, then data, desktops, cloud access, and peripheral devices.

5. Top Threats

Primary risks include IoT attacks, insider threats, malware/ransomware, and phishing-based credential compromise.

6. Backup & Restore Strategy

Smith’s Construction uses NAS daily/weekly backups and AWS encrypted off-site backups. Restore from NAS for local failures; restore from AWS for corruption, ransomware, or physical loss.

7. General Disaster Recovery Procedures

Steps include incident containment, verifying network integrity, preserving forensic evidence, rebuilding systems, restoring data, validating recovery, and documenting actions.

8. Incident-Specific Playbooks

IoT compromise: isolate, reset, update, segment.

Insider threat: disable access, secure workstation, investigate, restore files.

Malware/ransomware: isolate system, identify strain, reimage workstation, restore from backup.

Phishing: reset credentials, enable MFA, review logs, scan workstation.

9. Crisis Wind-Down

Perform forensics, communicate externally when needed, create post-incident reports, update cybersecurity controls, and conduct lessons-learned reviews.

10. Training & Exercises

DRP is distributed to all employees. Tabletop exercises annually; restore tests twice per year. DRP reviewed every 12 months or after an incident.