Ransomware Recovery Drill Runbook (SMB)

A repeatable, 60-90 minute tabletop + technical drill to prove you can restore critical operations. Use quarterly.

Scope

Pick **one laptop**, **one shared folder**, and **one SaaS app** (e.g., Microsoft 365, Google Workspace, Xero, Salesforce). The goal is evidence, not perfection.

Roles

Role	Responsibility
Incident Lead	Runs the timeline, makes go/no-go decisions, captures evidence.
IT Admin	Performs restores, confirms access controls, documents steps.
Business Owner	Defines what 'recovered' means (minimum viable operations).
Observer	Notes gaps, timing, and follow-ups (no blame).

Drill timeline

Time	Phase	What to do
T-0	**Declare scenario**	Simulate detection: 'Multiple endpoints encrypted; admin account suspected.'
T+5	**Contain**	Disable suspected account, isolate affected device(s), block risky access.
T+15	**Prioritize**	Name the 3 most critical business processes + owners.
T+25	**Restore test 1**	Restore one laptop or VM to a clean state.
T+45	**Restore test 2**	Restore one shared folder or file set from backup.
T+60	**SaaS recovery**	Re-issue MFA, rotate tokens, check mail rules/forwarding.
T+75	**Validate**	Business owner confirms core tasks work.
T+90	**Closeout**	Record RTO/RPO, gaps, and follow-ups.

Acceptance criteria (what 'good' looks like)

- [] You can disable a compromised account and force re-auth within 10 minutes.
- [] You can restore one endpoint to a clean state within 30 minutes (or have a known alternative).
- [] You can restore a representative set of files and validate integrity.
- [] You can prove backups are protected from the same admin account that manages day-to-day IT.
- [] You can produce a simple evidence pack (screenshots + timestamps).

Evidence to capture (attach to your baseline report)

Area	Example evidence
Identity	Screenshot of MFA enabled + sign-in logs showing account disabled/reset.
Backups	Screenshot of backup job success + immutable/offline setting if available.
Restore	Screenshot of restored endpoint version + restored files timestamp.
Admin separation	Proof daily account is not global admin / local admin.
Lessons learned	1 page: what broke, what to change, who owns it, by when.

Tip: If you cannot restore, you do not have a backup - you have a file-copy. This drill makes that visible early.