

# The Southern California Business Continuity Checklist

## Staying open through wildfire season, power shutoffs, earthquakes, and outages

Southern California doesn't get one kind of disruption — it gets all of them: Public Safety Power Shutoffs, wildfire smoke and evacuations, earthquakes, grid strain, and the cyberattacks that spike whenever a business is distracted. Continuity here isn't about predicting which one hits. It's about being able to keep operating when any of them does.

This is the checklist we walk our own clients through. Work down it honestly — every box you can't check today is a gap worth closing before the next red-flag warning.

### 1 Foundations (do these first, regardless of hazard)

- ☐ You have a written continuity / disaster-recovery plan, and someone owns it
- ☐ Backups run automatically for every critical system — and a restore was **tested** in the last 90 days (an untested backup is a hope, not a plan)
- ☐ At least one backup copy is **off-site / in the cloud**, not just on-premises
- ☐ You know your **RTO and RPO** — how fast you must be back, and how much data you can afford to lose — for each critical system
- ☐ A current contact list (staff, vendors, bank, insurer, IT) is reachable **without** your office network
- ☐ Someone can authorize decisions if the owner is unreachable

### 2 Power shutoffs (PSPS) & wildfire

- ☐ You're signed up for **SCE / LADWP outage and PSPS alerts** for every site address
- ☐ Critical on-site gear (firewall, switches, servers, phones) is on a **UPS** sized for a graceful shutdown — with a generator plan if you must stay live
- ☐ Core systems (email, files, line-of-business apps) are **cloud-hosted or cloud-failover capable**, so a dark office is not a dark business
- ☐ Staff can **work remotely on short notice** — laptops, secure remote access, and MFA already set up and tested
- ☐ Internet has a **failover path** (secondary line or cellular) for any site that must stay connected
- ☐ You've mapped which roles go fully remote vs. need a backup location, and staff know the plan before an evacuation order

### 3 Earthquake & physical-site risk

- ☐ Server / network equipment is physically secured (racks anchored, nothing that can topple)
- ☐ You can operate for 24–72 hours with your primary office inaccessible
- ☐ Critical data and systems do not depend on a single physical location
- ☐ Emergency procedures are posted and staff know the safe / assembly points

### 4 Communications & people

- ☐ A **notification tree** reaches every employee fast (text / app, not just email)
- ☐ Business phones (VoIP) can **forward or reroute** to mobiles or a remote team automatically
- ☐ Customers can reach you if the main office is down (published mobile line, status page, or answering service)
- ☐ Someone is designated to post customer updates so silence does not read as "closed for good"

### 5 Cybersecurity during disruption

- ☐ MFA is on for email, remote access, and financial systems (attackers target the chaos of an outage)
- ☐ Staff are briefed that **disaster-themed phishing and fake "IT support" calls spike** during regional events
- ☐ Remote access is through secured, monitored channels — not personal tools spun up in a hurry
- ☐ Endpoint protection and monitoring stay active on remote devices, not just office ones
- ☐ Wire-transfer and payment-change requests require **out-of-band verification**, especially during disruption

### 6 Recovery & proof

- ☐ You have run a **tabletop drill** — "the office is dark Monday, now what?" — in the last year
- ☐ A test restore has actually brought a critical system back, start to finish
- ☐ Vendor and cyber-insurance continuity / DR requirements are documented and met
- ☐ After any real event or drill, the plan gets updated with what you learned

#### How many boxes did you leave blank?

**0–3 unchecked** — strong shape. Keep testing.

**4–8 unchecked** — real exposure. Prioritize backups you have actually restored and remote-work readiness before the next PSPS season.

**9+ unchecked** — a single bad week could take you offline for days. Worth a focused plan now, while it is calm.

### We do this for a living — and we are local.

Pro Link Systems has kept Southern California businesses running through fire seasons, shutoffs, and outages since 1999, with a **24/7, US-based, in-house help desk** — real people who answer, live. Want a second set of eyes on the gaps above? We offer a **free 15-minute continuity review**: no pitch, just a straight read on where you are exposed and what to fix first.

**[prolinksystems.com/contact](https://prolinksystems.com/contact) • 1-800-890-6133**

*This checklist is general guidance, not a substitute for a continuity plan built for your specific systems, sites, and obligations.*