FOUNDER EMERGENCY KIT / 01

The first 72 hours

A practical response sequence. These are triage windows, not a promise that recovery finishes in three days.

First establish company authority, protect the live customer path, and prove that your team can operate, deploy, and recover without the departed developer.

0-2 HOURS

- [ ] Name the authorized decision owner and technical responder.
- [ ] Check login, checkout, customer access, alerts, and active incidents.
- [ ] Pause routine releases and destructive changes; record the last good deploy.

2-12 HOURS

- [ ] Inventory source, cloud, registrar/DNS, data, payments, messaging, and billing.
- [ ] Record company owner, admin, recovery email/phone, MFA holder, renewal.

12-24 HOURS

- [ ] Match the production release to repository history and an artifact.
- [ ] Locate backups and key owners; restore a recent copy in isolation.
- [ ] Identify deploy and rollback paths without testing on production.

24-48 HOURS

- [ ] Map human and machine access before controlled revocation or rotation.
- [ ] Reconcile a payment with webhook delivery and product access.
- [ ] Check queues, scheduled jobs, monitoring recipients, and renewals.

48-72 HOURS

- [ ] Separate blocked controls from unknown ones; rank by business consequence.
- [ ] Name the next owner, action, and review date for every material gap.
- [ ] Choose maintain, recover, stabilize, assess, hire, or modernize later.

Do not touch without review

Do not rotate every key, delete identities, shut down unfamiliar jobs, or merge a test deploy blindly.

Do not restore over production, access personal accounts, or approve a rewrite before mapping the live system.

Suspected compromise or malicious activity needs incident-response escalation and evidence preservation.

First-hour handoff notes

Authorized decision owner: _____

Technical responder: _____

Customer impact right now: _____

Last known good release: _____

Ownership inventory

Write account ownership and recovery paths here. Keep passwords, secrets, customer data, and private logs out of this worksheet.

CONTROL AREA	COMPANY OWNER / RECOVERY	PROOF / STATUS
Source control		
Cloud / hosting		
Domain / DNS		
Production database		
Backup / restore		
CI/CD		
Secrets		
Payments		
Email / SMS		
Monitoring		
Cron / queues		
Billing / renewals		

Evidence ladder - use the strongest true statement

CLAIMED Someone says access or a backup exists. No independent check yet.

PARTIAL Company account, recovery method, recent copy, or release record is visible.

VERIFIED An authorized second person performed a safe build, release-path check, or isolated restore.

For critical controls, record the proof location in your approved company workspace. A green dashboard or a zip file alone is not verified operational control.

FOUNDER EMERGENCY KIT / 03

Turn findings into action

A useful handover ends with named owners, evidence gaps, and the next safe step - not a vague green checklist.

Action owner / next step

CONTROL OR GAP	OWNER	NEXT SAFE ACTION	REVIEW

When to call for qualified help

- ☐ Active customer harm, suspected compromise, or an account you cannot lawfully access.
- ☐ No verified recent restore, unknown deployed revision, or payment-to-access failures.
- ☐ Conflicting ownership records or a replacement engineer who cannot establish a safe release path.

Choose the smallest supported next move

Maintain what works; arrange a bounded handover; recover company access; stabilize an active failure; hire a replacement; commission an independent assessment; or modernize in stages once recovery and rollback are proven.

Decision:

Why this is safe now:

Full guide and interactive checklist: techmitrise.com/insights/only-developer-left-first-72-hours/