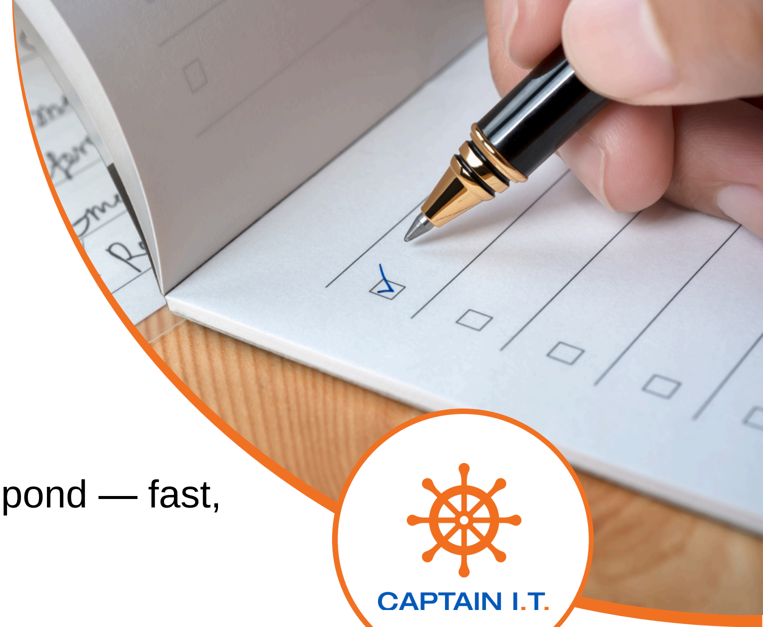

# CAPTAIN IT

## DISASTER RECOVERY CHECKLIST

When disaster strikes, here's how we respond — fast, clear, and with precision.

**Step 1:** **Initiate the Recovery Process**

- [ ] Alert the Captain IT Response Team (create internal ticket & Teams alert)
- [ ] Classify the event: outage, cyberattack, hardware failure, natural disaster, etc.
- [ ] Notify the Account Manager and Client Primary Contact
- [ ] Determine if client is on Compass, Anchor, or Captain Plan
- [ ] Document start time and who declared the event

**Step 2:** **Assess the Damage**

- [ ] Identify all affected systems (servers, shared drives, internet, etc.)
- [ ] Check if remote users are impacted
- [ ] Review recent alerts from the RMM, backups, and firewall logs
- [ ] Contact client to confirm what they're experiencing
- [ ] Document scope and initial impact in IT Glue ticket

**Step 3:** **Client Communication**

- [ ] Use pre-approved disaster email or call script
- [ ] Clearly explain the issue, what we're doing, and expected timeframe
- [ ] Set expectations for hourly or milestone-based updates
- [ ] Escalate to our leadership if a breach, data loss, or extended outage is suspected
- [ ] Notify third-party vendors if they are involved (e.g., internet, cloud apps)

**Step 4:** **Backup & Restore Operations**

- [ ] Access backup system (Datto, Axcient, or client-specific)
- [ ] Verify last successful backup
- [ ] Perform test restore before full recovery
- [ ] Restore data to known-good state or alternate location
- [ ] Rebuild key systems if needed (DC, file server, QuickBooks, etc.)
- [ ] Log restore times and files restored in ticket notes

**Step 5:** **System Recovery – Captain IT Priority Order**

- [ ] Domain Controllers / Active Directory
- [ ] File Shares and QuickBooks
- [ ] Line of Business Applications
- [ ] Microsoft 365 / Exchange
- [ ] Internet Access & DNS
- [ ] VPN / Remote Access
- [ ] Printers, scanners, VoIP phones
- [ ] Endpoint reimaging, if required

**Step 6:** **Security Response (If Cyber Incident)**

- [ ] Isolate compromised systems from the network
- [ ] Review FortiGate logs and SIEM (if enabled)
- [ ] Reset passwords for affected accounts
- [ ] Scan endpoints with SentinelOne or preferred EDR
- [ ] Coordinate with external IR vendor (if applicable)
- [ ] Begin forensic logging and save relevant logs

**Step 7:** **Client Access & Validation**

- [ ] Verify staff can log in to restored systems
- [ ] Confirm key business functions are working (accounting, email, cloud apps)
- [ ] Test printing, mapped drives, and remote desktop if applicable
- [ ] Schedule post-recovery follow-up with client
- [ ] Resume proactive monitoring & alerts

**Step 8:** **Internal Documentation**

- [ ] Update ticket with a full timeline
- [ ] Attach screenshots, restore logs, and backup confirmations to IT Glue
- [ ] Document client-specific lessons or weaknesses
- [ ] Flag issues for Quarterly Business Review (QBR)

**Step 9:** **Client Notification & Wrap-Up**

- [ ] Send "All Systems Operational" update to client
- [ ] Include summary of what happened and how it was resolved
- [ ] Advise on any suggested changes (e.g., upgrade firewall, add backup, implement MFA)
- [ ] Deactivate internal emergency mode
- [ ] Monitor all systems closely for the next 72 hours

**Step 10:** **Debrief & Improve**

- [ ] Hold internal post-mortem with team
- [ ] Review speed of response, communication, and restoration steps
- [ ] Update our playbooks, scripts, and client configurations
- [ ] Add topic to next team training or all-hands meeting
- [ ] Schedule DR test or tabletop for affected client within 30 days