XANTRION

TECH EXPERTS, ENDURING PARTNERS

Business Continuity Plan Sample

This sample business continuity plan shows how a firm can plan for a cybersecurity incident to ensure minimal loss of productivity.

Ransomware Scenario

Business overview: A 75-person professional services firm relies on Microsoft 365, a cloud file platform, line-of-business software, VoIP, and a managed IT provider.

Critical function: Client service delivery

Owner: Operations director

Maximum acceptable downtime: 8 hours

Dependencies: Email, file access, internet, CRM, finance platform

Risk scenario

Ransomware encrypts endpoints and shared files

Likely impact: Staff cannot access client documents or communicate reliably

Response lead: CIO or outsourced IT lead

Copywright 2026. Xantrion.

Response procedures

Issue identified by: Endpoint alerts and user reports

Incident declaration: IT lead confirms encryption activity and activates BCP

Immediate actions: Isolate affected devices, disable compromised accounts, notify leadership, preserve logs

Short-term workaround: Shift unaffected staff to clean devices, use alternate communications channel, prioritize active client deliverables

Recovery steps: Restore from clean backups, validate identity controls, communicate status updates, reset credentials, monitor for reinfection

Return to normal: Critical systems restored, users re-enabled, leadership approves closure

Communications

Internal lead: COO

External lead: Client services leader

Primary channels: Microsoft Teams and email

Backup channels: Mobile phones and SMS tree

Need Help?

Creating a business continuity plan is only part of the work. To be effective, it needs to reflect how your business actually operates, align with your IT environment, and be tested often enough to stay useful.

Contact us at 510-272-4701 or info@xantrion.com

Learn more at xantrion.com