

BUSINESS CONTINUITY & OPERATIONS PLAN

Plan Activation | Alternate Operations | IT & Data Recovery | HR & Staffing | Finance | Vendor
Continuity | Recovery

Business / Organization Name: _____	Primary Location / Address: _____
Prepared By: _____	Title / Role: _____
Date Prepared: _____	Last Updated: _____
Version #: _____	Approved By: _____
Plan Owner / BCP Coordinator: _____	Next Scheduled Review: _____
BIA Document Reference: _____	Emergency Operations Manual Version: _____

PURPOSE OF THIS PLAN

This Business Continuity & Operations Plan (BCP) defines how the organization will maintain or rapidly restore critical business functions during and after any disruptive event — including natural disasters, cyberattacks, facility loss, supply chain failure, key personnel loss, or public health emergencies. It is activated in conjunction with the Business Impact Analysis (BIA) Framework and the Crisis Communications & PR Playbook.

SECTION 1: PLAN OVERVIEW & GOVERNANCE

This section establishes the legal authority, scope, objectives, and governance structure of this Business Continuity Plan. All personnel listed here have defined responsibilities before, during, and after an activation event.

PLAN SCOPE & OBJECTIVES

This plan applies to:

All Locations Covered: _____ **Number of Employees Covered:** _____

All Departments Covered: _____ **Geographic Region(s):** _____

Exclusions / Out of Scope: _____

Primary Objectives of This Plan:

1. Protect the health, safety, and welfare of all employees and stakeholders
2. Maintain or restore Tier 1 Critical Business Functions within defined RTOs
3. Minimize financial losses and operational disruption
4. Protect the organization's data, assets, and reputation
5. Meet all legal, regulatory, and contractual obligations during disruption

BCP GOVERNANCE TEAM

These individuals are responsible for maintaining, testing, and activating this plan. Each role must have a trained backup who can fulfill all responsibilities in the primary's absence.

Role / Title	Assigned Person	Cell Phone	Email	Backup Person	Backup Phone	Primary Responsibility

PLAN MAINTENANCE & TESTING SCHEDULE

Activity	Frequency	Responsible Party	Last Completed	Next Due Date	Notes / Findings

Business Resilience OS

Activity	Frequency	Responsible Party	Last Completed	Next Due Date	Notes / Findings

Required activities: Full plan review (annual), Tabletop exercise (annual), Communication tree test (semi-annual), IT backup/restore test (quarterly), Alternate site readiness check (annual), Staff training (annual onboarding + annual refresher).

PLAN ACTIVATION AUTHORITY

Scenario / Threat Level	Who May Declare a BCP Event	Who Must Be Notified Within 1 Hour	Authorization Method

SECTION 2: PLAN ACTIVATION & INCIDENT RESPONSE

This section details the exact steps taken from the moment a disruptive event is recognized through the formal declaration of a BCP activation. Speed and clarity of initial response dramatically reduce total recovery time.

THREAT & HAZARD IDENTIFICATION MATRIX

Rate each threat for Likelihood (1=Rare, 5=Highly Likely) and Impact (1=Minor, 5=Catastrophic). Multiply to get the Risk Score. Prioritize mitigation for any score above 12.

Business Resilience OS

Threat / Hazard Type	Likelihood (1–5)	Impact (1–5)	Risk Score	Existing Controls / Mitigation	Mitigation Action Needed
Natural Disaster (hurricane, flood, tornado, earthquake)					
Fire or Explosion					
Extended Power Outage					
Cyberattack / Ransomware					
Data Breach					
Key Personnel Loss (death, sudden resignation)					
Critical Vendor / Supplier Failure					
Pandemic / Public Health Emergency					
Civil Unrest / Active Threat					
IT / Technology System Failure					
Supply Chain Disruption					
Regulatory / Legal Action					

BCP ACTIVATION DECISION TREE

STEP 1

DETECT & ASSESS

An event occurs or is anticipated. The first aware employee notifies their direct manager immediately. The manager notifies the BCP Coordinator within 15 minutes. Document the time, nature, and scope of the incident.

STEP 2

INITIAL SEVERITY ASSESSMENT

The BCP Coordinator assesses: (a) Is life safety threatened? → Contact 911 immediately. (b) Are Tier 1 Critical Business Functions impacted or threatened? (c) Is recovery within normal operations possible, or is BCP activation required?

STEP 3

NOTIFY LEADERSHIP

If BCP activation may be required, the BCP Coordinator immediately notifies the Incident Commander (CEO / Owner) and the full BCP Governance Team. Do not wait for full information — notify immediately.

STEP 4	FORMAL ACTIVATION DECISION The Incident Commander makes the formal go/no-go decision to activate this BCP. If activated: issue all-hands notification, convene the first situation call within 60 minutes, and begin executing section-specific continuity protocols.
STEP 5	EXECUTE CONTINUITY PROTOCOLS Each section lead executes their assigned continuity protocols as documented in Sections 3–8 of this plan. The Incident Commander maintains command. Status updates every 4 hours for first 24 hours.
STEP 6	MONITOR & ESCALATE / DE-ESCALATE Continuously reassess the situation. Escalate resource requests as needed. De-activate BCP when Tier 1 functions are restored and sustained for 48+ hours.

INCIDENT LOG — ACTIVATION RECORD

Date / Time	Event / Action	Reported By	Decision Made	Authorized By	Next Action

BCP ACTIVATION CHECKLIST — FIRST 60 MINUTES

IMMEDIATE ACTIONS (0–30 Minutes)	FIRST HOUR ACTIONS (30–60 Minutes)
☐ Confirm life safety of all personnel	☐ Convene emergency leadership call

Business Resilience OS

- | | |
|---|--|
| <ul style="list-style-type: none">☐ Account for all employees at affected location(s)☐ Contact 911 if life safety is threatened☐ Notify BCP Coordinator of incident☐ Begin incident documentation log☐ Assess immediate facility access / safety☐ Notify Incident Commander (CEO / Owner)☐ Do NOT make public statements — no social media☐ Preserve all evidence and documentation☐ Activate phone tree / notification system | <ul style="list-style-type: none">☐ Formally declare BCP activation if warranted☐ Assign section leads to continuity roles☐ Issue all-staff emergency notification☐ Notify key clients if service is impacted☐ Notify insurance carrier of potential claim☐ Contact legal counsel☐ Activate alternate work locations if needed☐ Begin IT damage assessment and recovery☐ Set next status update time — no more than 4 hrs |
|---|--|

SECTION 3: ALTERNATE OPERATIONS & WORK LOCATION CONTINUITY

When the primary location is unavailable, operations must shift immediately to a pre-planned alternate. This section identifies all alternate work locations, remote work protocols, and minimum staffing requirements to keep Tier 1 functions operating.

ALTERNATE WORK LOCATION REGISTRY

Location Name / Type	Address	Capacity (# Staff)	Available Within	Key Contact	Phone	Functions Supported

Location types: Secondary owned facility, leased co-working space, hotel conference room, key employee homes, client site (if permitted), cloud-based virtual operations. Identify at least TWO alternate locations.

REMOTE WORK CAPABILITY ASSESSMENT

Department	# Employees Who Can Work Remotely	Remote Work % of Normal Capacity	Equipment Provided By Company?	VPN / Secure Access Available?	Gaps / Limitations

MINIMUM OPERATING REQUIREMENTS — BY TIER

Define the absolute minimum resources required to keep each Tier 1 and Tier 2 function operational. This drives the alternate location setup and IT recovery priorities.

Business Function	Priority Tier	Min. # Staff Required	Required Systems / Software	Required Equipment	Acceptable Alternate Method

Business Function	Priority Tier	Min. # Staff Required	Required Systems / Software	Required Equipment	Acceptable Alternate Method

SCENARIO-SPECIFIC OPERATIONS PROTOCOLS

SCENARIO A — LOSS OF PRIMARY FACILITY (Fire, Flood, Structural Damage)

Primary Alternate Location: _____ **Activation Time Target:** _____

Facility Access Contact: _____ **Security / Alarm Code Location:** _____

Immediate Actions:

- ☐ Verify all personnel have evacuated safely and are accounted for
- ☐ Contact property insurance carrier immediately — document all damage
- ☐ Engage general contractor / restoration company from approved vendor list
- ☐ Redirect all phone lines to alternate number or mobile
- ☐ Activate alternate work location — notify all staff within 2 hours
- ☐ Retrieve off-site backup data and critical documents

Estimated Cost of Temporary Relocation Per Day \$: _____

Insurance Policy # for Property Damage: _____

SCENARIO B — EXTENDED POWER OUTAGE (12+ Hours)

Generator Location / Capacity: _____ **Fuel Supply / Vendor:** _____

Utility Company Name: _____ **Outage Reporting Phone:** _____

Immediate Actions:

- ☐ Activate UPS (Uninterruptible Power Supply) on all critical servers immediately
- ☐ Start generator — verify fuel level and capacity
- ☐ Prioritize generator power: servers, POS systems, communications, lighting
- ☐ Report outage to utility company — get estimated restoration timeline
- ☐ Activate remote / alternate work for staff if outage exceeds 4 hours
- ☐ Check and protect any temperature-sensitive inventory or equipment

Generator Capacity (kW): _____ **Max Runtime on Full Tank:** _____

Fuel Supplier / Emergency Fuel Delivery Contact: _____

SCENARIO C — PANDEMIC / PUBLIC HEALTH EMERGENCY

Remote Work Activation Threshold: _____ % Staff Min. Required On-Site: _____

Immediate Actions:

- ☐ Monitor official health guidance (CDC, state/local health dept.) daily
- ☐ Activate remote work protocols for all non-essential on-site roles
- ☐ Establish daily wellness check-in protocol for all staff
- ☐ Increase cleaning and sanitization frequency at all locations
- ☐ Identify cross-trained backups for all Tier 1 function personnel
- ☐ Establish contactless delivery / service options for customers
- ☐ Communicate clearly and regularly with staff, clients, and vendors

HR / Leave Policy Document Location: _____

SECTION 4: IT, DATA & CYBERSECURITY CONTINUITY

Technology failure — whether from a cyberattack, hardware failure, or natural disaster — is the most common trigger for BCP activation. This section documents your data backup strategy, system recovery procedures, and cybersecurity incident response.

CRITICAL SYSTEMS INVENTORY

System / Application Name	Business Function Supported	Hosted Where?	Recovery Priority (Tier 1–3)	RTO	RPO	IT Contact / Vendor

Business Resilience OS

System / Application Name	Business Function Supported	Hosted Where?	Recovery Priority (Tier 1–3)	RTO	RPO	IT Contact / Vendor

DATA BACKUP STRATEGY

Primary Backup Solution / Platform: _____	Backup Frequency: _____
Backup Storage Location (Cloud / Physical): _____	Off-Site Backup Location: _____
Backup Verified / Tested (Frequency): _____	Last Successful Restore Test: _____
IT Manager / Vendor: _____	IT Emergency Phone: _____
Cloud Provider(s): _____	Account # / Portal URL: _____

SYSTEM RECOVERY PROCEDURES

For each Tier 1 system, document the exact recovery procedure. Who does what, in what order, and how long it should take.

System Name	Recovery Method (Restore / Failover / Rebuild)	Person Responsible	Step-by-Step Procedure Location	Estimated Recovery Time	Dependencies Before This Step

System Name	Recovery Method (Restore / Failover / Rebuild)	Person Responsible	Step-by-Step Procedure Location	Estimated Recovery Time	Dependencies Before This Step

CYBERSECURITY INCIDENT RESPONSE

CYBER INCIDENT — IMMEDIATE RESPONSE RULE

If a cyberattack, ransomware, or unauthorized data access is suspected: (1) DO NOT pay any ransom without legal and cybersecurity counsel. (2) DO NOT attempt to fix or remove malware yourself — you may destroy forensic evidence. (3) Isolate affected systems IMMEDIATELY by disconnecting from the network. (4) Notify legal counsel and cyber insurance carrier before making any public statement.

STEP 1

ISOLATE

Immediately disconnect affected devices from all networks (Wi-Fi, LAN, VPN). Do not power off — this preserves forensic evidence.

STEP 2

NOTIFY

Alert IT lead, BCP Coordinator, CEO, legal counsel, and cyber insurance carrier within 30 minutes. Document exact time of discovery.

STEP 3

ASSESS SCOPE

Determine what systems are affected, what data may have been accessed or exfiltrated, and what the entry point was. Engage cybersecurity firm if needed.

STEP 4

REGULATORY NOTIFICATION

Assess breach notification obligations under HIPAA, PCI-DSS, state privacy laws, or other applicable regulations. Consult legal counsel on timing.

STEP 5

RESTORE FROM CLEAN BACKUP

Rebuild affected systems only from verified clean backups. Do not reconnect until all systems are confirmed clean by your IT provider.

STEP 6

POST-INCIDENT HARDENING

Patch the vulnerability, reset all credentials, enable multi-factor authentication, and conduct a full security audit within 30 days.

Cybersecurity Insurance Carrier: _____	Policy #: _____
Cyber Incident Response Firm: _____	24/7 Emergency Phone: _____
Data Breach Legal Counsel: _____	Phone: _____
IT Forensics Vendor: _____	Phone: _____

SECTION 5: HR, STAFFING & PERSONNEL CONTINUITY

People are the most critical and most vulnerable asset in any business continuity event. This section ensures the organization can maintain essential staffing levels, protect employee welfare, and fill critical knowledge gaps when key personnel are unavailable.

KEY PERSONNEL SUCCESSION PLAN

For every role that supports a Tier 1 or Tier 2 function, there must be a trained backup who can perform all critical responsibilities. Identify the gap if no backup currently exists.

Critical Role / Title	Current Person	Cell Phone	Backup Person 1	Backup Phone	Backup Person 2	Cross-Training Complete?

KNOWLEDGE TRANSFER & CRITICAL

DOCUMENTATION

Document all critical knowledge that exists only in one person's head — logins, processes, vendor relationships, or system knowledge. This is a Single Point of Failure risk.

Critical Knowledge / Process	Currently Held By	Document Location	Backup Person Trained?	Knowledge Transfer Target Date

EMERGENCY STAFFING PROTOCOLS

MANDATORY STAFF REDUCTION SCENARIO	KEY PERSON LOSS SCENARIO (Sudden Departure / Incapacitation)
☐ Identify minimum staff required per Tier 1 function ☐ Prioritize retention of cross-trained employees ☐ Implement remote work for all possible roles ☐ Reduce non-essential hours before Tier 1 roles ☐ Contact staffing agency for temporary workers ☐ Document all decisions — consult HR / attorney ☐ Communicate transparently with all staff ☐ Review payroll obligations and cash requirements	☐ Activate pre-designated backup immediately ☐ Retrieve all credentials and documentation from secure vault ☐ Brief backup on all pending projects and deadlines ☐ Notify key clients if client-facing role is affected ☐ Engage recruiter for permanent replacement if needed ☐ Review outstanding contracts or agreements they managed ☐ Assess all system accesses and reassign or revoke ☐ Conduct knowledge-capture interview if planned departure

EMPLOYEE SUPPORT & WELFARE PROTOCOLS

Employee Assistance Program (EAP) Provider: _____	EAP Phone / Portal: _____
HR Manager / Contact: _____	HR Emergency Phone: _____
Payroll Continuity Commitment (describe): _____	Payroll Provider Emergency Contact: _____
Workers' Compensation Carrier: _____	Claims Phone: _____
Mental Health Resource (Crisis Line): _____	Employee Communication Platform: _____

All employees must be informed about pay continuity, benefits status, work location, and expected return-to-work timeline within the first 24 hours of any BCP activation.

SECTION 6: FINANCE & CASH FLOW CONTINUITY

A business can survive almost any crisis if it has cash. This section ensures financial resources are accessible, obligations are protected, and emergency funding options are identified before they are needed.

EMERGENCY FINANCIAL RESOURCES

Resource Type	Institution / Provider	Account # / Reference	Available Amount \$	Access Method	Authorization Required	Contact / Phone

Business Resilience OS

Include: Operating checking accounts, Business line of credit, Business credit cards, Emergency reserve fund, SBA disaster loan pre-qualification, Key-person insurance payout, Business interruption insurance proceeds.

FINANCIAL OBLIGATIONS PROTECTION PLAN

Refer to the Accounts Payable section of the Master SOP for the full payment priority list. Document specific steps to protect each critical obligation below.

Financial Obligation	Monthly Amount \$	Protection Strategy	Who Manages During Crisis	Emergency Contact at Payee

BUSINESS INTERRUPTION INSURANCE

Carrier Name: _____	Policy Number: _____
Coverage Limit \$: _____	Waiting Period (Days): _____
Monthly Benefit \$: _____	Covered Perils: _____
Claims Phone (24/7): _____	Agent Name: _____
Agent Phone: _____	Agent Email: _____
What Must Be Documented to File Claim: _____	Exclusions to Note: _____

EMERGENCY SPENDING AUTHORIZATION

Expense Category	Normal Approval Limit \$	Emergency Authorization Limit \$	Who Can Authorize	Documentation Required

All emergency expenditures above \$500 must be documented with a brief written justification, receipt, and authorization signature. This documentation is required for insurance claim submission.

SECTION 7: VENDOR & SUPPLY CHAIN CONTINUITY

Supply chain disruptions are among the fastest-growing causes of business continuity events. This section identifies backup vendors for every critical input, establishes pre-negotiated emergency procurement options, and defines communication protocols with key suppliers.

CRITICAL VENDOR CONTINUITY MATRIX

Critical Input / Service	Primary Vendor	Primary Phone	Backup Vendor	Backup Phone	Max Days Without (Before Impact)	Emergency Stock / Buffer

Business Resilience OS

Critical Input / Service	Primary Vendor	Primary Phone	Backup Vendor	Backup Phone	Max Days Without (Before Impact)	Emergency Stock / Buffer

EMERGENCY PROCUREMENT PROTOCOLS

IF PRIMARY VENDOR FAILS	IF SUPPLY CHAIN IS BROADLY DISRUPTED
☐ Contact backup vendor immediately ☐ Check current inventory levels for buffer time ☐ Notify operations and production leads ☐ Assess impact on open customer orders ☐ Issue force majeure notice to vendor if applicable ☐ Contact insurance for supply chain coverage ☐ Brief sales team on any delivery timeline changes ☐ Document all actions for insurance / legal purposes	☐ Activate all pre-identified alternate vendors ☐ Assess 30/60/90-day inventory buffer on all critical inputs ☐ Consider emergency bulk purchasing if budget allows ☐ Identify substitute products or raw materials ☐ Communicate proactively with all affected customers ☐ Escalate to senior leadership if supply cannot be restored ☐ Assess contract obligations and force majeure clauses ☐ Monitor industry news and peer company responses

KEY VENDOR COMMUNICATION PLAN

Vendor Name	Service / Product	Primary Contact	Phone	Notification Trigger	Preferred Communication Method	Account / Contract #

Business Resilience OS

Vendor Name	Service / Product	Primary Contact	Phone	Notification Trigger	Preferred Communication Method	Account / Contract #

SECTION 8: COMMUNICATIONS CONTINUITY

Communication failure during a crisis amplifies every other problem. This section ensures all internal and external communication channels remain functional and that critical contacts can be reached regardless of what systems are down. Reference the Crisis Communications & PR Playbook for full external messaging templates.

COMMUNICATION SYSTEMS BACKUP PLAN

Communication System	Primary Use	Current Status (Operational / At-Risk)	Backup System If Primary Fails	Backup Contact / Access Method

Business Resilience OS

Systems to address: Main office phone, Employee mobile phones, Email (Exchange / Google), Video conferencing (Zoom / Teams), Slack / internal messaging, Website / web hosting, Physical mail / courier, ERP / CRM systems.

EMPLOYEE NOTIFICATION TREE

In the event of a BCP activation, the following notification tree must be executed within the first 30 minutes. Each person is responsible for reaching those below them in the tree.

Notification Level	Person / Role	Cell Phone	Email	Notified By	Notification Method	Backup If Unreachable

EXTERNAL STAKEHOLDER NOTIFICATION PRIORITIES

Stakeholder Group	Notification Priority (1 = First)	Notification Method	Who Sends	Template Location	Timing Requirement

Stakeholder Group	Notification Priority (1 = First)	Notification Method	Who Sends	Template Location	Timing Requirement

Stakeholder groups: Priority clients, All customers (mass notification), Key vendors, Insurance carrier, Legal counsel, Board / investors, Regulatory agencies (if required), Media (via spokesperson only).

SECTION 9: RECOVERY, RESTORATION & RETURN TO NORMAL OPERATIONS

Recovery begins the moment the immediate crisis is stabilized. This section defines how the organization transitions from emergency operations back to normal business — systematically, safely, and with full documentation.

RECOVERY PHASE OVERVIEW

Phase	Name	Objective	Timeframe (Typical)	Key Activities
PHASE 1	IMMEDIATE RESPONSE	Protect life safety; contain damage; activate BCP	0 – 24 Hours	Evacuation, notification, incident command
PHASE 2	CRISIS MANAGEMENT	Maintain Tier 1 operations via alternate means	24 Hrs – 7 Days	Alternate location, remote work, customer comms
PHASE 3	BUSINESS RECOVERY	Restore normal operations progressively by tier	1 – 4 Weeks	System restoration, facility repair, staffing
PHASE 4	FULL RESTORATION	Return to full pre-event operational capacity	2 – 8 Weeks	Process verification, performance monitoring
PHASE 5	POST-INCIDENT REVIEW	Capture lessons learned; update BCP	Within 30 Days	Debrief, BCP update, staff recognition

RECOVERY TASK TRACKER — BY FUNCTION

Business Function	Priority Tier	Recovery Task	Assigned To	Target Completion	Actual Completion	Status (Not Started / In Progress / Complete)

RETURN-TO-NORMAL-OPERATIONS CRITERIA

DE-ACTIVATION STANDARD

The BCP may be formally de-activated only when ALL of the following criteria are met and sustained for a minimum of 48 consecutive hours: (1) All Tier 1 Critical Business Functions are fully operational. (2) All personnel are at standard work locations OR an approved remote/alternate arrangement has been confirmed as permanent. (3) All customer commitments are being met at normal service levels. (4) IT and data systems are fully restored and verified. (5) All legal, regulatory, and insurance notifications have been completed.

De-Activation Criterion	Met? Y / N	Date Confirmed	Confirmed By	Notes

Business Resilience OS

De-Activation Criterion	Met? Y / N	Date Confirmed	Confirmed By	Notes

POST-INCIDENT REVIEW CHECKLIST

Complete this review within 30 days of BCP de-activation. Assign owners to every finding. Update this plan before the next annual review.

INTERNAL DEBRIEF & LESSONS LEARNED	PLAN UPDATES & FUTURE PREVENTION
☐ Conduct full debrief with BCP Governance Team ☐ Document timeline of all events and decisions ☐ Identify what worked well — capture and formalize ☐ Identify what failed or was missing from the plan ☐ Assess all RTOs — were they met? ☐ Assess financial impact vs. insurance coverage ☐ Survey all staff for feedback on the response ☐ File all insurance claims and document outcomes ☐ Review all vendor and partner performance ☐ Acknowledge and celebrate team performance	☐ Update this BCP with all lessons learned ☐ Close all identified gaps from BIA gap analysis ☐ Update vendor backup list based on experience ☐ Improve cross-training for any roles that failed ☐ Schedule a tabletop exercise within 90 days ☐ Update emergency contact list if changes occurred ☐ Review and increase insurance coverage if needed ☐ Implement any technology improvements identified ☐ Update BIA to reflect any new functions or risks ☐ Set new BCP review date and assign owner

POST-INCIDENT FINANCIAL SUMMARY

Total Days BCP Was Active: _____	Date BCP Formally De-Activated: _____
Total Revenue Lost (Estimated) \$: _____	Total Recovery Costs Incurred \$: _____
Business Interruption Insurance Claimed \$: _____	Insurance Payout Received \$: _____
Net Financial Impact \$:	Facilitator of Post-Incident Review:

_____	_____
-------	-------

SECTION 10: EXECUTIVE SIGN-OFF & ANNUAL PLAN APPROVAL

This Business Continuity & Operations Plan has been reviewed, approved, and authorized by the executive team listed below. By signing, each approver confirms they understand their responsibilities under this plan and authorize its implementation.

DOCUMENT CONTROL & VERSION HISTORY

Version	Date	Updated By	Approved By	Summary of Changes

ANNUAL REVIEW SIGN-OFF

This plan must be formally reviewed and re-approved at least once per year, or immediately following any BCP activation event, major organizational change, or significant revision to the Business Impact Analysis.

Name / Title: _____	Department: _____
Signature: _____	Date: _____

Name / Title: _____	Department: _____
Signature: _____	Date: _____

Name / Title: _____	Department: _____
Signature: _____	Date: _____

Business Resilience OS

Name / Title: _____	Department: _____
Signature: _____	Date: _____

This is a living document.

Review annually. Update after every BCP activation. Distribute to all Section Leads. Store one printed copy at each work location and one off-site. Keep the most current digital version in a cloud location accessible to the full BCP Governance Team.