GENERAL BCP BUSINESS CONTINUITY PLAN

Organization: [ORGANIZATION LEGAL NAME] (Corporation) **Primary Address:** [PRIMARY BUSINESS ADDRESS] **Industry:** [INDUSTRY BUSINESS DESCRIPTION] **Plan Version:** 1.0 **Effective Date: Primary State of Operations:** [STATE] **Next Mandatory Review:** Annual

---

Document Control

| Field | Value | |---|---| | Plan Owner | [PLAN OWNER BCP COORDINATOR NAME], Business Continuity Coordinator | | Plan Owner Contact | [PLAN OWNER EMAIL] · [PLAN OWNER 24 7 PHONE] | | Executive Sponsor | [EXECUTIVE SPONSOR NAME], Chief Executive Officer | | Version | 1.0 | | Effective Date | | | Review Cadence | Annual |

Confidentiality. This Plan is a confidential business document of [ORGANIZATION LEGAL NAME]. It contains sensitive information about operations, personnel, vendors, and recovery strategies. Distribution is restricted to authorized personnel and regulators with a need to know.

---

1. Purpose and Scope

This Business Continuity Plan (the "Plan") documents the strategies, procedures, and resources [ORGANIZATION LEGAL NAME] (the "Organization") will use to maintain and recover its critical business functions in the event of a significant disruption. The Plan is designed as an all-hazards framework covering events including, but not limited to: Power Outage; Cyberattack; Natural Disaster; Pandemic; and any other event that materially impairs the Organization's ability to operate.

The Plan applies to all employees, contractors, officers, and directors of the Organization at all locations, and to the Organization's critical third-party service providers to the extent contractually required.

ISO 22301:2019 Alignment. This Plan is designed to align with the principal requirements of ISO 22301:2019 (Societal security — Business continuity management systems — Requirements), including leadership commitment, business impact analysis, risk assessment, strategy selection, exercise and testing, and continual improvement.

2. Governance and Roles

2.1 Plan Ownership

The **Business Continuity Coordinator** ([PLAN OWNER BCP COORDINATOR NAME]) owns this Plan, coordinates its maintenance and testing, and reports to the **Executive Sponsor**, [EXECUTIVE SPONSOR NAME] (Chief Executive Officer). The Plan Owner is authorized to convene the Crisis

Management Team and to approve expenditures reasonably necessary to execute the Plan during an incident, subject to the Executive Sponsor's review for expenditures above any delegation limit.

2.2 Crisis Management Team (CMT)

| Role | Primary | 24/7 Contact | |---|---|---| | CMT Lead | [CRISIS MANAGEMENT TEAM LEAD NAME] | [CRISIS TEAM LEAD 24 7 PHONE] | | Plan Owner / BCP Coordinator | [PLAN OWNER BCP COORDINATOR NAME] | [PLAN OWNER 24 7 PHONE] | | Executive Sponsor | [EXECUTIVE SPONSOR NAME] | — | | IT / Technology Lead | [IT TECHNOLOGY LEAD NAME] | [IT LEAD 24 7 PHONE] | | Communications / PR Lead | [to be assigned] | — | | HR Lead | [to be assigned] | — | | Legal Counsel | [to be assigned] | — |

2.3 Activation Authority

Any member of the CMT may recommend activation; the **CMT Lead** (or designee) is authorized to activate the Plan. Full activation triggers the notification procedures in §6 and convenes the CMT within thirty (30) minutes (virtually or physically).

3. Business Impact Analysis (BIA)

3.1 Critical Business Functions

The following functions have been identified as critical to the Organization's mission and continued operation:

[LIST CRITICAL BUSINESS FUNCTIONS ONE PER]

3.2 Recovery Objectives

| Metric | Target | Description | |---|---|---| | **Recovery Time Objective (RTO)** | **24 hours** (twenty-four) | Maximum time to restore critical functions after activation. | | **Recovery Point Objective (RPO)** | **4 hours** (four) | Maximum tolerable data loss, measured in time. | | **Maximum Tolerable Downtime (MTD)** | **72 hours** | Duration beyond which the disruption threatens organizational viability. | | **Estimated Financial Impact** | **$0.00 / day** | Net operating loss per day of full disruption. |

3.3 Key Dependencies

[Critical dependencies to be documented in the BIA workbook maintained by the Plan Owner.]

4. Threats Addressed

This Plan addresses, at a minimum, the following threat categories: **Power Outage**; **Cyberattack**; **Natural Disaster**; **Pandemic**; . Threat-specific playbooks are maintained as appendices and reviewed on the cadence set forth in §10.

5. Recovery Strategies

5.1 Alternate Work Site

The Organization's alternate work-site strategy is **Remote**.

5.2 Data Backup and Recovery

Data backups follow a **Cloud Daily** strategy, retaining backups for **90 days**. Backup integrity is verified at least monthly; full restoration from backup is tested at least annually.

5.3 Cyber Insurance

The Organization maintains cyber liability insurance with ****, policy no. ****. In the event of a cyber incident, the Plan Owner or CMT Lead shall notify the carrier via its incident hotline () as soon as reasonably practicable and in any case before engaging outside counsel, forensics, or ransom-negotiation vendors not pre-approved by the carrier, to preserve coverage.

6. Communications and Notification

6.1 Internal Notification

The Organization will notify employees using: Sms; Email; Phone Tree; .

6.2 External Communications

All public and media statements shall be issued solely by the authorized spokesperson (as designated by the CMT Lead) in coordination with Legal Counsel. Employees shall not speak to the media without authorization and shall redirect inquiries to the spokesperson.

6.3 Customer Notification

Customers will be notified of disruptions that materially affect service, using the Organization's customer communication channels. Notifications will be reviewed by Legal Counsel before release.

7. Incident Response Procedures

Phase 1 — Detection and Assessment (0–1 hr). Incident reported to Plan Owner or CMT Lead. Initial triage: life safety, scope, affected systems, likely duration. Activation decision made.

Phase 2 — Activation and Notification (1–4 hr). CMT convenes; roles confirmed. Employees, key customers, regulators (as required), insurers, and vendors notified. Communications plan initiated.

Phase 3 — Stabilization and Recovery (4 hr – RTO). Containment of damage. Activation of alternate work site, failover to backup systems, supply substitution. Continuous status updates every 2–4 hours.

Phase 4 — Restoration (post-RTO). Return to normal operations. Decommission temporary workarounds. Decontamination / forensic preservation as needed.

Phase 5 — Post-Incident Review. Within 30 days of all-clear, the Plan Owner shall deliver a written After-Action Report to the Executive Sponsor identifying root cause, timeline, response effectiveness, gaps, and corrective actions. Corrective actions shall be tracked to closure.

8. Regulatory Framework

CIRCIA (6 U.S.C. §681b)

If the Organization qualifies as a covered entity in a critical infrastructure sector under CIRCIA rulemaking, it shall report covered cyber incidents to CISA within 72 hours and any ransom payment within 24 hours.

OFAC Ransomware Advisory

Payments to sanctioned persons or jurisdictions in response to ransomware may violate the International Emergency Economic Powers Act and the Trading with the Enemy Act. No ransom payment shall be authorized without (a) screening against OFAC SDN and sectoral sanctions lists, (b) consultation with Legal Counsel, (c) notification to and coordination with the FBI and CISA, and (d) approval from the Executive Sponsor.

OSHA General Duty Clause (29 U.S.C. §654)

The Organization shall furnish a place of employment free from recognized hazards likely to cause death or serious physical harm. Emergency action plans (29 C.F.R. §1910.38) are maintained for each facility.

ADA / Title VII Accommodation

Plan implementation shall comply with the Americans with Disabilities Act and Title VII, including reasonable accommodations for disability and sincerely held religious beliefs, and shall not be implemented in a discriminatory manner.

9. Standards Alignment

This Plan is aligned with **NIST SP 800-34 Rev. 1** (Contingency Planning Guide for Federal Information Systems). It is further aligned with the **NIST Cybersecurity Framework 2.0** functions of Govern, Identify, Protect, Detect, Respond, and Recover.

10. Testing, Training, and Maintenance

Exercises. The Organization will conduct the following exercises on at least an annual basis: Tabletop; Functional; . Results are documented in After-Action Reports.

Training. All employees receive awareness training on this Plan at **Annual** cadence. CMT members receive role-specific training annually.

Plan Maintenance. The Plan is reviewed and updated on a **Annual** basis, and additionally after any material change in operations, significant incident, or regulatory change.

11. Approval

Plan Owner / BCP Coordinator

______________________________ PRINTED NAME

______________________________ SIGNATURE

______________________________ DATE

Executive Sponsor

______________________________ PRINTED NAME

______________________________ SIGNATURE

______________________________ DATE

This Plan is a living document. Report gaps, errors, or suggested improvements to [PLAN OWNER BCP COORDINATOR NAME] ([PLAN OWNER EMAIL]).