BUSINESS CONTINUITY PLAN (BCP)

1. PURPOSE

This Business Continuity Plan (BCP) provides the framework for sustaining critical business operations during a cyber incident or other disruptive event. It complements the Incident Response Plan (IRP) and Disaster Recovery Plan (DRP).

2. SCOPE

This BCP includes all personnel, systems, networks, devices, and business processes whose interruption would significantly impact the organization.

3. ROLES AND RESPONSIBILITIES

• Business Owner / Executive Leadership: Activates continuity procedures and communicates major decisions.

• IT Director: Assesses infrastructure, activates continuity environments, and coordinates technical response.

• Security Engineer: Maintains and tests continuity systems, ensures secure access.

• Managers: Coordinate staff duties and support the transition to continuity operations.

• Employees: Follow guidance, access continuity systems securely, and maintain professional conduct during crisis operations.

4. COMMUNICATION CHANNELS

Primary: Corporate email, messaging platform, internal phone tree.

Secondary: Emergency SMS list, personal email (if primary systems unavailable).

Third-Party Communication: Cloud providers, MSPs, hosting vendors.

5. BUSINESS IMPACT ANALYSIS SUMMARY

Critical assets prioritized for continuity include:

• Identity and authentication systems

• File storage and document systems

• Line-of-business applications

• Cloud systems supporting operations

• Company endpoints required for productivity

6. RISK OVERVIEW

Primary risks to business continuity include ransomware, major server failure, network outages, cloud misconfigurations, data corruption, and physical disasters affecting the main office.

7. CONTINUITY METHODS

• Cloud-Based Alternate Site hosting mirrored critical servers.

• Pre-imaged spare laptops containing essential applications.

• Hot spare hardware for rapid replacement of failed components.

• Cloud storage with continuous synchronization for all employees.

• Secure VPN or cloud access gateway for remote connectivity.

8. EMPLOYEE ACCESS DURING CONTINUITY

Employees will:

1. Receive formal notification of continuity activation.

2. Obtain pre-imaged laptops if needed.

3. Work from home or designated alternate sites.

4. Access business applications and files through cloud-hosted platforms.

9. TRANSITION PROCEDURES DURING A CRISIS

1. Business owner declares continuity activation.

2. IT Director isolates compromised infrastructure.

3. Managers distribute instructions to staff.

4. Security Engineer enables continuity platform access.

5. Employees switch to remote operations following IR playbooks.

10. RESTORATION AND RETURN TO NORMAL OPERATIONS

• IT restores the primary infrastructure per the DRP.

• Leadership notifies employees when on-site operations resume.

• Continuity devices are collected and sanitized before reuse.

11. PLAN STORAGE AND DISTRIBUTION

Stored securely in an encrypted cloud repository and distributed to leadership, IT, and security teams. Offline encrypted copies retained for emergency use.

12. TESTING AND MAINTENANCE

• Annual full continuity simulation.

• Quarterly testing of spare hardware and cloud access.

• After-action reviews following crisis events to identify improvement opportunities.

END OF DOCUMENT