WALSIN LIHWA CORPORATION

Business Continuity Management Policy

Document Number: A-2-TP-IT-112000-001
Effective Date: 2022/09/27

1. Responsibilities

1.1 Business Continuity Management Unit

1.1.1. All critical systems of Walsin Lihwa shall have business continuity management operations, with a designated responsible person assigned by the department director of the critical system.

1.1.2. Assess risks and threats to information system services and IT business operations, formulate business continuity strategies, and establish business continuity plans.

1.1.3. Regularly test and review existing business continuity plans, revising them based on test results to maintain effectiveness.

1.1.4. Review the appropriateness of business continuity plans and their test results.

1.1.5. Conduct various activities as required, such as drills, training, and reviews for continuous improvement.

2. Operations and Management

2.1 Business Continuity Management

2.1.1. The Information Center serves as the highest command unit when initiating the company’s business continuity plan, assisting in resource allocation and executing internal coordination and communication.

2.1.2. The BCM team shall assess the impact of information system service interruptions, determine the Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO), and Recovery Point Objective (RPO), and perform Business Impact Analysis (BIA).

2.1.3. The BCM team shall adopt appropriate continuity strategies based on the level of impact to information system services.

2.2 Establishing the Business Continuity Plan

2.2.1. Formulation

2.2.1.1. Define the company’s “critical management systems” (SAP, MES) and formulate continuity plans.

2.2.1.2. Develop a BCM framework, scenario descriptions, and procedures in the “Business Continuity Plan Drill & Handling Report” for execution, adjustment, and drills.

2.2.1.3. Scenarios may be set based on business experience or past information security incidents.

2.2.1.4. Response measures must meet the required service levels.

2.2.2. Drills

2.2.2.1. Conduct at least one continuity plan drill annually for a critical system.

2.2.2.2. Drills require approval from the section manager and may include tabletop exercises, notification drills, or recovery drills.

2.2.2.3. Results shall be documented in the “Business Continuity Plan Drill & Handling Report” and reviewed by the section manager.

2.2.3. Maintenance

2.2.3.1. Review plans annually and update as needed to align with internal/external requirements, business process changes, organizational adjustments, or system modifications.

2.2.3.2. Consider factors such as new equipment, detection/control technologies, personnel changes, facility relocation, application changes, operational changes, legal changes, cost-effectiveness, and resource needs.

2.2.4. Awareness & Training

2.2.4.1. When required, BCM training shall be provided to explain drill details and ensure participant understanding.

2.3 Execution Management

2.3.1. If service interruption persists despite incident response efforts, the section manager may decide to activate the BCM plan.

2.3.2. Ensure designated backup resources are available; the Information Center resolves any shortages.

2.3.3. BCM team shall coordinate external communications.

2.3.4. Record all execution processes in the “Business Continuity Plan Drill & Handling Report.”

2.3.5. Post-incident, prepare improvement plans and written reports.

2.4 Monitoring, Audit, and Improvement

2.4.1. Within one month after incident resolution, review all stages—notification, response, recovery—to evaluate achievement of objectives and convene a review meeting.

2.4.2. If plan progress is delayed, present review and improvement proposals to the Information Security Promotion Team.