HIWIN IT Security Business Continuity Plan

1. Purpose

Establish a comprehensive information security business continuity management mechanism and formulate specific response plans to ensure rapid response and damage reduction in the event of catastrophic incidents, cyber attacks, or system failures. This will maintain the continuity of critical business operations and protect the confidentiality, integrity, and availability of the company's information assets, effectively reducing the impact of emergencies.

2. Scope

Applicable to information systems, network equipment, data centers, cloud services, and related personnel within the scope of the Information Security Management System (ISMS), as well as outsourced cooperation units.

3. Responsibilities

A. Information Department

Conduct business impact analysis.

Responsible for updating the information business continuity plan.

Plan the information business continuity plan/disaster recovery plan.

Assist in organizing relevant education and training.

B. Operations Monitoring and Incident Handling Team (hereinafter referred to as the Incident Handling Team)

Execute the information business continuity plan/disaster recovery plan.

Determine the severity of incidents, conduct preliminary handling of emergencies or abnormal events, and report the handling situation to the information security management representative.

For the composition of this team, please refer to the "Information Security Incident Management Specification."

C. Information Security Management Representative

Review the information business continuity plan/disaster recovery plan.

Supervise the information business continuity plan/disaster recovery plan.

Decide the severity of incidents and initiate relevant information business continuity plans.

4. Risk Assessment and Business Impact Analysis (BIA)

A. Risk Identification:

Conduct comprehensive assessments of natural disasters (earthquakes, typhoons), human factors (hacker attacks, internal abuse), and technical failures (system crashes, data loss). To properly plan the information business continuity plan, the following items should be considered in conjunction with business units:

- Identify critical business operations.
- Tolerable downtime for each business activity (Recovery Time Objective, RTO).
- Tolerable data loss period for each business activity (Recovery Point Objective, RPO).
- Resources and budget required for operational recovery.

B. Impact Analysis:

Assess the impact of various incidents on operations, finance, regulatory compliance, and reputation, and classify them based on the degree of impact. Based on the results of the impact analysis, consider cost-effectiveness factors, conduct feasibility analysis of response plans, and then formulate the information business continuity plan based on the assessment results.

C. Identification of Key Resources:

The results of the business impact analysis should determine the resources for priority activities, such as critical business operations, including ERP systems, customer databases, email servers, network equipment, etc.

5. Response Mechanism and Recovery Strategy

A. Data Backup and Offsite Redundancy:

Perform daily data backups and store them at the offsite redundancy center.

Adopt RAID architecture and cloud redundancy mechanisms for critical systems.

B. System Recovery Plan (DRP):

Set RTO (Recovery Time Objective) and RPO (Recovery Point Objective).

Activate the backup system within 4 hours after a disaster occurs and restore critical business within 24 hours.

C. Communication and Coordination Mechanism:

Establish a Cyber Security Incident Response Team (CSIRT) composed of the information department, legal department, and senior management.

Activate emergency communication mechanisms, including phone, email, and instant messaging tools.

6. Information Security Incident Reporting and Handling Process

A. Incident Detection and Preliminary Reporting

Employees who discover system abnormalities, intrusions, or suspicious information security behaviors can report abnormal events to the IT department or information security mailbox or extension via internal email or phone.

B. Incident Confirmation and Classification

Confirm whether it is an information security incident.

C. Classification handling:

Minor incidents/false alarms: Simple reporting and closure.

Second-level and above incidents: Initiate complete handling process, may need to issue major announcements.

D. Initiate Response Plan

Departments involved in initiating the information security incident response plan include:

- Intellectual Property Department, Legal Department
- Operations Monitoring and Incident Handling Team
- Information Security Management Representative
- Company Spokesperson
- External resources (such as professional vendors)

7. Incident Handling Process

Handling Stages	Description
Judgment and Analysis	Confirm the nature of the incident, scope of impact, and whether it involves confidential information.
System Setup/Adjustment/Response Measures	Includes isolation, elimination, system recovery, etc.
Investigation and Forensics	Conduct incident forensics and trace the source.
Improvement and Tracking	Propose improvement measures and track

Handling Stages	Description
	implementation effectiveness.
Stock Exchange Major Announcement (if conditions are met)	If the incident meets the criteria for major information disclosure, the company spokesperson will issue the announcement.
Closure and Learning	Complete the incident report, incorporate it into education and training, and system improvement.

8. External Support

If the incident is complex or has significant impact, external information security professional vendors may be invited to assist in handling.

9. Employee Training and Drills

Information Security Awareness Training:

- Conduct at least one company-wide information security training annually, covering password management, social engineering prevention, reporting processes, etc.
- New employees are provided with information security education when they join the organization.

10. BCP Drills:

Conduct simulation drills every six months, including scenarios such as system interruptions, data leaks, disaster recovery, etc.

Conduct effectiveness evaluation and improvement suggestions after the drills.

Continuous Improvement and Audit Mechanism

11. Internal Audit:

The information department conducts an internal audit once a year to review the effectiveness and compliance of plan drills.

The audit report is submitted to the annual management review meeting of the Information Security Committee.

12. External Certification:

Regularly undergo external audits by third-party certification bodies for ISO 27001:2022.

The execution results of the plan drills are disclosed in the sustainability report.

13. Public Disclosure and Stakeholder Communication

A. Disclosure Channels:

The execution results of this plan drill have been disclosed in the sustainability report and its dedicated public website.

Provide stakeholders with access and feedback mechanisms.

B. Communication Mechanism:

Major information security incidents will be proactively reported to the competent authorities and affected parties as required.