HCL Software

Business Continuity Management Policy

Policy Statement

HCLSoftware is committed to establishing, maintaining, and regularly testing a comprehensive Business Continuity Management System (BCMS) to ensure the resilience of its operations against various threats. We recognize that unforeseen events can disrupt our ability to deliver products and services, and we are dedicated to proactive planning and rapid response to mitigate such impacts.

This policy mandates the development and implementation of robust Business Continuity Plans (BCPs) for all critical functions, ensuring the safety of our personnel, the integrity of our data, and the continuity of our customer-facing services.

Scope

This policy applies to all aspects of our business operations critical to the design, development, delivery, maintenance, and support of our software products and services. It covers all personnel, systems, data, and processes within HCLSoftware, as well as our interactions with third-party vendors and partners.

Our Commitment:

1. **Business Impact Analysis (BIA):** A Business Impact Analysis (BIA) is conducted periodically (at least annually) and after significant organizational or product changes to:
    - Identify Critical Business Functions
    - Assess Impact of Disruption
    - Determine Recovery Time Objectives (RTOs)
    - Determine Recovery Point Objectives (RPOs)
    - Identify Dependencies
    - Identify Critical Resources

2. **Risk Assessment:** A comprehensive risk assessment is performed to identify potential threats and vulnerabilities to critical business functions and assets.
   This includes:
    - Threat Identification
    - Vulnerability Analysis
    - Likelihood and Impact Analysis
    - Mitigation Strategies

3. **Business Continuity Plan (BCP):** Based on the BIA and Risk Assessment, detailed BCPs are developed for each critical business function.
   Each BCP includes:
    - Activation Criteria
    - Incident Response Procedures
    - Disaster Recovery Procedures
    - Recovery Strategies

- Resource Requirements
- Communication Protocols
- Roles and Responsibilities
- Escalation Procedures
- Deactivation Procedures

4. **Crisis Management and Incident Response:** A Crisis Management Team (CMT) is established and trained to manage and coordinate the overall response to a significant disruptive event.
   The CMT is responsible for:
   - Incident Assessment
   - Decision Making
   - Coordination
   - Communication
   - Post-Incident Review

5. **Communication Strategy:** Effective communication is paramount during a disruption.
   Our communication strategy includes:
   - Internal Communication
   - External Communication
   - Emergency Contact Information Repository

6. **Training and Awareness:** All employees receive appropriate training and awareness regarding the Business Continuity Policy and their specific roles within the BCP.
   This includes:
   - Initial Training
   - Refresher Training
   - Role-Specific Training
   - Awareness Campaigns

7. **Testing and Review:** Business Continuity Plans (BCPs) are regularly tested to ensure their effectiveness and identify areas for improvement.
   BCPs are tested at least annually, or more frequently if significant changes occur (e.g., new product launches, major system upgrades, organizational restructuring).
   Types of Tests:
   - Tabletop Exercises: Discussion-based exercises to walk through BCP steps.
   - Simulation Exercises: Realistic exercises involving simulated disruptions.
   - Full-Scale Drills: Comprehensive tests involving actual system failovers and recovery procedures where feasible.

   A thorough review is conducted after each test to document lessons learned, identify deficiencies, and update the BCPs accordingly.

8. **Audit:** Our Business Continuity Management System is certified to ISO 22301 Standards. Our BCMS is subject to independent internal and external audits periodically as per ISO Standards to ensure compliance with this policy and best practices.

9. **Outsourced Critical Systems**: When a Business Unit (BU) begins the selection process to outsource a critical system to a third-party vendor, the BU ensures that they select a vendor that has a BCP or a DR procedure with an acceptable SLA.

Policy Review and Updates

This Business Continuity Policy will be reviewed and updated by Senior Management at least annually, or as needed, to reflect changes in the organization, its risk profile, technology, regulatory requirements, or lessons learned from incidents or tests.