*IT Business Continuity Policy*

Table of Contents

[Purpose 1](#_Toc5047307)

[Scope 1](#_Toc5047308)

[Policy 1](#_Toc5047309)

[Business Impact Analysis 1](#_Toc5047310)

[Recovery Planning Support 2](#_Toc5047311)

[System Criticality Rating 2](#_Toc5047312)

[Plan Development 3](#_Toc5047313)

[Personnel Management 3](#_Toc5047314)

[Plan Communication 3](#_Toc5047315)

[Plan Testing 3](#_Toc5047316)

[Recovery Personnel 3](#_Toc5047317)

[Recovery and Restoration 4](#_Toc5047318)

[Violations 4](#_Toc5047319)

[Definitions 4](#_Toc5047320)

[References 5](#_Toc5047321)

[Related Documents 5](#_Toc5047322)

[Approval and Ownership 5](#_Toc5047323)

[Revision History 5](#_Toc5047324)

Purpose

This policy defines the requirements for developing, testing, and maintaining the CompanyX (the “Company”) business continuity plan.

Scope

This policy applies to all CompanyX information assets and facilities, with a target audience of CompanyX management, Information Technology employees and Third-Parties.

Policy

### Business Impact Analysis

**Business Impact Analysis** - The Information Security Department or its designee must perform a business impact analysis (BIA) each year after the annual organization-wide risk assessment.

**Business Impact Analysis** **Requirements** - At the very least, the business impact analysis BIA must result in the specification of the following:

* Downtime - the maximum period that CompanyX can go without critical information processing services,
* Recovery Period - the time period in which management must decide whether to move to an alternative processing site,
* Recovery State - the minimum acceptable production information systems recovery configuration.
* Loss Analysis - analysis of the financial losses potentially incurred during the outage,
* Risk Analysis - a qualitative residual risk assessment
* Asset Criticality Rating - asset criticality analysis.

**Business Impact Analysis – Individual Production Systems** - As part of the systems development cycle, all computer information systems must be evaluated by Information Security specialists to determine the minimum set of controls, the cost/benefit of such controls and the budget required to mitigate and maintain risk at a level acceptable to the business process(es) involved.

**Mission Critical Systems And Refurbished/Reconfigured Equipment** - Information systems equipment which has been refurbished, or which has gone through an extensive reconfiguration process, must not be used for CompanyX mission critical systems unless it has been expressly approved for this purpose by the Information Security Manager.

### ****Recovery Planning Support****

**Standardized Support Requirements** - All subsidiaries, divisions, departments, and other CompanyX organizational units that require support by the Information Technology Department on a priority basis in the event of an emergency or a disaster must implement hardware, software, policies, and related procedures consistent with CompanyX requirements.

**Business Interruption Support Levels** - Each year, user department management and Information Technology Department management must agree upon and document the support levels that will be provided in the event of a disaster or emergency.

**Coverage For Every Critical Application And Infrastructure Component** - Every critical production business application and every production information systems infrastructure component (voicemail, private branch exchange switch, web page server, etc.) must include measures in the contingency plan that permits the restoration of service within the time period specified in the RTO.

**Recovery Time Objectives** – The CompanyX business Continuity Plan must include specific Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each information system according to the system classification rating. The default recovery time is 72 hours for production systems.

### ****System Criticality Rating****

**Multi-User Application Criticality Rating** - In conjunction with the Information Owners, Information Systems Department managers must periodically prepare or revise an assessment of the degree of criticality of all production multi-user computer applications.

**Five Category Rating System -** All production computer applications must be placed into one of five criticality classifications, each with separate handling requirements: highly critical, critical, priority, required, and deferrable. This criticality classification system must be used throughout CompanyX, and must form an integral part of the system contingency planning process.

### Plan Development

**Business Contingency Plans - Management must prepare and periodically update a Business Continuity (Recovery) Plan (BCP) that specifies how alternative facilities (offices, telephones, copiers, etc.) and systems will be provided so workers can continue operations in the event of a business interruption.**

**Reversion To Manual Procedures** - If CompanyX critical business activities could reasonably be performed with manual procedures rather than computers, a manual computer contingency plan must be developed, tested, periodically updated, and integrated into Information system contingency plans.

**Recovery Procedures** - Procedures for restoring service must be documented in formal contingency plans which are reviewed, tested, and updated at least annually.

### Personnel Management

**Occupant Emergency Plan (OEP)** - An Occupant Emergency Plan will be included as part of overall business continuity planning within CompanyX.  This plan will focus on personnel safety in the face of physical threats, which include, but are not limited to, exposure to hazardous materials (whether chemical or biological), sudden weather events (tornadoes, severe thunderstorms, etc.), bomb threats, violence at the workplace, and fires.  These procedures will include directions for either evacuation or sheltering-in-place.

### Plan Communication

**Plan Availability** - Business and information systems contingency plans must be continuously accessible over the Internet through at least two separate Internet addresses that are supported by different Internet service providers.

**Plan Classification and Communication** - CompanyX's information systems contingency plans are classified as “Internal Use Only”, and they must not be disclosed to Third-Parties without prior approval from the Information Security Manager.

### ****Plan Testing****

**Contingency Plan Testing** - To the extent practical and feasible, Information system contingency plans must be tested annually to assure that they are still relevant and effective. Each such test must be followed by a brief report to top management detailing the results of the test and any remedial actions that need to be taken.

**Telephone Number Testing** – As part of contingency plan testing, Information Security Department staff must test and revise a call tree indicating every available telephone number for every worker involved in information-systems-related contingency planning, as well as disaster and emergency response.

### Recovery Personnel

**Recovery Personnel Notifications** – Every worker who has responsibility for business recovery must be notified of his/her responsibilities and corresponding work requirements **Recovery Assignment** – System recovery plans and procedures must specifically assign responsibility for managing and facilitating the restoration of service.

**Recovery Personnel Training** - All designated workers must receive sufficient training and practice to allow them to expediently follow these same procedures and successfully restore the involved service.

**Recovery Personnel Rotation** - The workers who participate in off-site recovery operations with CompanyX information systems must be rotated regularly so that at all times at least two people will have the technical knowledge needed to perform each essential recovery task.

**Contingency Planning And Recovery Roles Review** - The roles and responsibilities for both information systems contingency planning and information systems recovery must be reviewed and updated annually by the Information Security Manager.

### Recovery and Restoration

**Data Synchronization During System Restoration** - In the event of multiple production system failure, the data inputs and outputs of interdependent systems must be carefully synchronized and verified before returning these systems to production status.

**Return to Normal (Production) Status** - Before returning any Information system which falls under the aegis of legal or regulatory requirements back to production, the system must be validated or certified according to those requirements. The proper management must sign off on the validation or certification as specified by the applicable requirements.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. CompanyX reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. CompanyX does not consider conduct in violation of this policy to be within an employee’s or Third-Party’s course and scope of employment, or the direct consequence of the discharge of the employee’s or Third-Party’s duties. Accordingly, to the extent permitted by law, CompanyX reserves the right not to defend or pay any damages awarded against employees or Third-Parties that result from violation of this policy.

Any employee or Third-Party who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

Definitions

**Business Continuity Plan (BCP)** - The documentation of a predetermined set of instructions or procedures that describe how an organization’s business functions will be sustained during and after a significant disruption.

**Business Impact Analysis (BIA)** - A management level analysis, which identifies the impacts of losing company resources. The BIA measures the effect of resource loss and escalating losses over time, in order to provide senior management with reliable data upon which to base decisions on risk mitigation and continuity planning.

**Information Asset** - Any CompanyX data in any form, and the equipment used to manage, process, or store CompanyX data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and Third-Party data.

**Recovery Time Objective (RTO)** – The specific time interval during which systems must be restored to production status. High-availability systems may require recovery times that are almost instant, while other systems may be recovered in longer time periods such as 24 or 72 hours.

**Recovery Point Objective (RPO)** – The specific time in the past that system state must be recovered. For example, production systems may be required to recover to a point no longer than 24 hours prior to the system interruption.

**Third-Party** - Any non-employee of CompanyX who is contractually bound to provide some form of service to CompanyX.

References

ISO/IEC 27002: 17.1 Information security continuity

NIST: CP-1 Contingency Planning (CP)

PCI-DSS: 12.10.1 Incident Response Plan – Continuity

US-CSF: RC.RP: Recovery Planning

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Policy Author | Title | MM/DD/YYYY |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title | MM/DD/YYYY |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | 10/05/2019 | MM/DD/YYYY |  |
|  |  |  |  |  |