Frank Cowan Company

Information System Disaster Recovery and Business Continuity Policy

Instructions

This template is a starting point to enable you to create an Information Systems Business Continuity Policy tailored to meet the needs of your organization.

This policy is intended to address business continuity for information systems only and should be part of a comprehensive Business Continuity Policy that addresses all of the business functions necessary for the continued effective operation of your organization.

Information systems recovery may, or may not, provide adequate recovery of the data sets required for business operations. Whether or not data recovery is included in information systems recovery processes, a separate Data Backup and Disaster

Recovery plan is required in order to ensure that critical business data is protected from all threats.

Please refer to the accompanying guide Creating an Information Systems Disaster Recovery and Business Continuity Plan for background and general information about information systems business continuity planning.

Perform a full document replacement of **<Organization>** with the proper name of your organization.

When you have customized the policy to your satisfaction, you can simply delete these instructions and paste the remaining text into your own policy document format. Alternatively, you may modify the footer in this document to suit your organization.

Policy Change Log

Date	Change	Edited by:	Approved by:
	Policy creation		

Table of Content

Instructions 1
Policy Change Log 1
Purpose of the Policy 3
Scope of the Policy 3
Definitions 3
Responsibility for Policy Implementation 4
Policy Requirements 4
Communication of the Policy 4
Policy violations and non-compliance 4
Information System Disaster Recovery and Business Continuity Plan 4
System Recovery Plan: Primary Business Application 5
Name of System Recovery Plan 6

Purpose of the Policy

The purpose of this policy is to establish processes to ensure the availability of all information systems required for essential business operations in the event of an equipment failure, service disruption, or a loss of operational capacity resulting from a fire or natural disaster.

Scope of the Policy

This policy applies to all <Organization> devices, employees, and contractors. All employees and contractors with access to <Organization> computing devices or information systems shall comply with this policy as it applies to their job duties.

Definitions

Information system is defined as a system that is required to process information used in business operations. An information system includes all of the hardware, operating system software, application software, network connections, and external services required for proper operation.

Business mission-critical system is defined as an information system that is required to support essential business functions during both normal operations and during a disaster or other event that may limit the organization's capacity to conduct normal operations. Some business functions may not be mission-critical if loss of these system functionality does not adversely affect the organization's ability to conduct essential business operations.

Off-site location is defined as a physical location that is geographically distant from the production location such that no single weather-related or other disaster would be likely to affect both locations.

Public or Private "cloud" is defined as a collection of hardware and software that is located in a secure location with redundant systems for power and Internet connectivity. Public clouds are multi-tenant data centers where computing infrastructure can be purchased at a required capacity, on either a temporary or permanent basis. Private clouds are owned by the organization or an affiliate and are not available to the general public.

External services are defined as services that are provided by an external provider, such as a power company or Internet Service Provider (ISP).

Restore Service Level (RSL) is defined as the required capacity of an information system for minimal or interim operations. If a system operating at 50% of its normal operating capacity is adequate to support minimal business operations during a failure or disaster event, then the RSL is 50%.

Maximum Tolerable Downtime (MTD) is defined as the maximum amount of time that an information system can remain non-functional before business operations are adversely affect.

Restore Time Objective (RTO) is defined as the time required to restore an information system from its maintained (backup) state to the Restore Service Level, establish connectivity, and make it available for business operations.

Restore Point Objective (RPO) is defined as the maximum amount of data loss that can be tolerated in terms of time. If the RPO is 1 hour, then restore points must be created on an hourly basis.

Recovery Initiation Point (RIP) is the time when recovery should be initiated. This typically occurs when the time since system failure plus the Recovery Time Objective is equal to the Maximum Tolerable Downtime. For example, if the Recovery time objective is 1 hour and the Maximum Tolerable Downtime is 5 hours, recovery should be initiated 4 hours after system failure. RIP can also be expressed as MTD minus RTO.

Responsibility for Policy Implementation

The <Organization> Security Officer or other authorized representative shall be responsible for ensuring implementation of all items listed in the Policy Requirements section. Responsibility for the creation and implementation of specific procedures may be assigned to internal staff or contractors as appropriate.

Policy Requirements

The <Organization> Security Officer or other authorized representative shall ensure compliance with the following standards:

1. Data Backup and Disaster Recovery Plan: The Security Office shall create and maintain a Data Backup and Disaster Recovery Plan to ensure proper backup and recovery of critical business data. This is required even if data recovery is included in the Information Systems Disaster Recovery and Business Continuity Plan. The Data Backup and Disaster Recovery Plan may refer to the Information Systems Disaster Recovery and Business Continuity plan as part of one or more Data Backup Plans.
2. The Recovery Time Objective must always be less than the Maximum Tolerable Downtime.
3. All servers and data storage devices shall be protected by Uninterruptable Power Supply (UPS) devices to protect against power fluctuations and short-term disruptions.
4. All UPS devices shall be configured to send shutdown signals to all servers and data storage devices, allowing sufficient time to allow for proper shutdown.
5. Where possible, external services should be redundant (e.g. multiple ISP connections, on-site power generators, etc.)

Communication of the Policy

The <Organization> Security Officer shall communicate this policy to appropriate individuals as necessary to ensure proper implementation.

Policy violations and non-compliance

Intentional violations of this policy shall subject the violator to appropriate sanctions. These sanctions may include suspension or dismissal.

Policy non-compliance shall result in a written warning for the first violation. Subsequent sanctions will be at the discretion of the Security Officer.

Information System Disaster Recovery and Business Continuity Plan

[Instructions: Below is an example of a typical system recovery plan for a system named “Primary Business Application”. This example plan is for the local recovery of the Primary Business Application within 4 hours with a maximum data loss of 1 hour. In the event of a disaster that renders the entire network unusable (such as a fire, flood, or extended power outage), the plan also provides for off-site recovery of the system in the outsourced IT service provider’s data center within 8 hours with a maximum data loss of 4 hours. Your recovery plan may not have the same requirements and may be more or less complex. You may need multiple business continuity plans for different systems. Below the example is a recovery plan template that you can copy. For more information, please refer to the accompanying guide Creating an Information Systems Disaster Recovery and Business Continuity Plan].

System Recovery Plan: Primary Business ApplicationName of Data Set

Who is Responsible for configuration and management of recovery software and hardware?	IT Systems Inc. Network Operation Center
Who is Responsible for monitoring production system and initiating recovery processes?	IT Systems Inc. Network Operation Center
Who is responsible for managing recovery process?	IT Systems Inc. Network Operation Center
What Business applications are supported by this system?	Primary Business Application
What hardware and software components are required for system operation?	Domain controller, SQL Server, virtual switch
What is the Recovery service level (RSL) for this system?	50%
What is the Maximum Tolerable Downtime (MTD) for this system?	4 hours for local recovery, 8 hours for cloud recovery
What is the Recovery Time Objective (RTO) for this system?	45 minutes for local recovery and 2 hours for cloud recovery
What is the Recovery Point Objective (RPO) for this system?	1 hour for local recovery and 4 hours for cloud recovery
What is the Recovery Initiation Point (RIP) (MTD – RTO = time to initiate recovery) for this system?	3 hours 15 minutes for local recovery and 6 hours for cloud recovery
Describe the plan details and how objectives will be met in the space below	
IT Systems Inc. is an outsourced IT services provider that operates a Network Operations Center (NOC) and a data center. IT Systems Inc. is responsible for managing this system recovery plan and all recovery processes.	
The Primary Business Application requires the availability of two Microsoft Windows servers and network connectivity. A Domain controller must be available so users can authenticate to the Microsoft SQL server that hosts the application. Backup and recovery software running on the two production servers replicates to virtual machine images of the servers which are running on a Backup and Recovery Device installed in the server room. These images are updated hourly. These images are then replicated to the IT Services Inc. data center and updated every 4 hours. The NOC receives notice when any component of the Primary Business Application System is not functioning as expected and initiates recovery as per the plan. In the event that either or both servers has failed, but the local network is still operational, the recovery virtual machine image(s) will be connected to the network. Data loss could be as much as 1 hour. In the event that both servers have failed, the recovery images will be running at approximately 50% of production capacity. Users will access the application from the local network as they normally would. In the event the entire network has failed, as a result of an extended power outage or a natural disaster, the virtual images of the two servers are brought online at the IT Services Inc. data center. These servers will be able to communicate through a virtual switch at the data center. Users will be able to connect to the Primary Business Application from any computer, using an IP address and instructions that will be posted on Disaster Recovery page of the company website. Users will be able to download and install the client application. Once the client application has been installed, all features of the Primary Business Application will be available and business operations can continue.	

Name of System Recovery Plan

Who is Responsible for configuration and management of recovery software and hardware?	
Who is Responsible for monitoring production system and initiating recovery processes?	
Who is responsible for managing recovery process?	
What Business applications are supported by this system?	
What hardware and software components are required for system operation?	
What is the Recovery service level (RSL) for this system?	
What is the Maximum Tolerable Downtime (MTD) for this system?	
What is the Recovery Time Objective (RTO) for this system?	
What is the Recovery Point Objective (RPO) for this system?	
What is the Recovery Initiation Point (RIP) (MTD – RTO = time to initiate recovery) for this system?	
Describe the plan details and how objectives will be met in the space below	