CONTINUITY AND RECOVERY PLANNING GUIDE

The Continuity Planning process is designed to assist an organization in determining action plans for disaster recovery or incident response. The process also aids businesses in estimating the cost of recovery from a disaster or incident.

The Business Continuity Plan is designed to educate staff on the goals and process of continuing business operation in light of a disaster or incident. In writing a departmental business continuity plan, one should consider the following:

- Potential revenue loss
- Incurring extra expenses
- Compromised customer service
- Loss of confidence impact
- Implementation process for the Business Continuity plan

The disaster recovery plan stems from the Business Continuity plan, as disaster recovery procedures are the first vital step in maintaining business operation after a disaster or incident. The disaster recovery plan should detail the following:

- Maintenance of any secondary equipment/facilities
- Data backup technique and procedures
- Access control for all temporary systems
- Implementation process for the disaster Recovery plan

The Business Continuity and Disaster Recovery plans are designed to provide the organization with general procedures for recovery. Specific steps for execution should be included in the plans, as they serve as instructional guides to staff in the event of a disaster. The distribution of these documents, however, should be limited to those involved with the implementation of Business Continuity and Disaster Recovery procedures.

In the following pages of this document, sample Business Continuity and Disaster Recovery plans are presented. Each organization will have different technology requirements and business structure. The sample documents are not applicable to every environment. Although the Business Continuity and Disaster Recovery Plan documents appear similar, the Disaster Recovery document is usually more technical and details specific information technology requirements for IT staff.
SAMPLE BUSINESS CONTINUITY PLAN

Widget Department
Business Continuity Plan

**Plan Objectives**
In the event of a disaster that affects the Widget Department’s ability to function as a provider of goods and services to the community, this Business Continuity Plan, along with the accompanying Disaster Recovery Plan, will be used to ensure continuation of the Widget Department’s rudimentary business operations. The scope of this plan includes widget rentals, widget sales, returns, inventory management and reconciliation of sales/rental values. The goals of the plan include strategies to address the following:

1. Minimizing revenue loss after disaster
2. Contain expense due to disaster
3. Reduce any compromise of customer service
4. Reduce any loss of confidence from customers

This Business Continuity Plan will be reviewed annually and revised as business and information technology environments change. The plan, along with the Disaster Recovery plan will be tested as part of annual Incident Response testing to ensure that responsible staff are prepared in the event of a disaster.

**Continuity/Recovery Staff Responsibilities**
Staff representing the Accounting Office, Business Office, and the Information Technology Office of the Widget Department will be required to execute the Business Continuity and Disaster Recovery Plans in the event of a disaster. Each Office will designate staff to be trained and test the plans annually. All designated staff will rotate job roles in plan testing to ensure that plans are properly executed in the event of a disaster.

Designated staff are as follows:
1. Jane – IT Office – 575-XXXX
2. Bob – Accounting – 575-XXXX
3. Joe – Business – 575-XXXX

The duties of the IT Office representative include executing the Disaster Recovery Plan to restore the minimal necessary IT resources needed to continue operation in a limited capacity until a full recovery can be made.

The duties of the Accounting Office representative include ensuring all financial resources, including cash/check received, are secured away from the disaster site and confidentiality of customer financial data is maintained until cash/check payments can be properly receipted. Any financial assets of the Widget Department will be managed by the Accounting Office representative and another designee, determined by upper management at the time of the disaster, until a full recovery can be made.

The Business Office representative is responsible for protecting the intellectual assets of the Widget Department and maintaining customer service during the disaster. Recurring customers will receive notice from the Widget Department via telephone or email that our operation has temporarily changed location or level of immediate service due to a disaster, but that operation will continue. Customers will be provided with the alternate business location and contact information to continue business.
**Disaster Operation Procedures**

The Widget Department has a secondary operation location that is capable of supporting full business operation, including inventory storage, fax/telephone capabilities and Ethernet capabilities for computer use. The IT Office representative and Disaster Recovery team will ensure that staff can access the inventory management system, customers can access the Widget Department’s website and orders can be processed. Procedures for Disaster Recover are described in the Disaster Recovery Plan document.

Operation at the secondary location will continue until it is deemed safe to return to the primary location and the Disaster Recovery team of the IT Office has restored Information Technology resources needed for full business operation back to the primary location. Customers will be notified of the return to full business operation capacity and that Widget Department has returned to the primary facility.

The time-frame of a full business recovery is dependent on the nature of the disaster, and in many cases, this Business Continuity Plan may not be fully implemented if the disaster is small in nature. The goal is to have a full recovery implemented as soon as possible, given the nature of the disaster. The aforementioned Disaster Recovery Plan details recovery procedures for the following disasters:

- Loss of system or facility resources (hardware failure or power outage) – Fail-over to secondary nodes using the virtualization fail-over function. Fail-over can be completed in 15 minutes and full business operation continued. Once the primary equipment/resources are restored, fail-back to the primary system will be completed.

- Destruction of primary facility—Remove business operations to secondary facility permanently if secondary facility is suitable. If the secondary facility cannot maintain full business capacity long-term, begin searching for a new primary facility.

**Business Continuity Inventory Information**

The secondary facility currently contains the following equipment in order to maintain business operations in the event of a disaster.

1. 10 – Dell Vostro 320 FT10 workstations
2. 3 – HP LaserJect P1505N network printers
3. 2 – Dell PowerEdge M905 servers with a total of 6 virtual machines
4. 1 – Netgear ProSecure UTM25
5. 1 – HP 3180 Fax
6. 1 – Canon ImageCLASS D1105 copier
7. 4 – IBM SurePOS 300 Express cash registers

Inventory is recorded in the Accounting module of the Widget Department’s inventory management system by serial number and model number. If equipment from the primary location fails, equipment from the secondary location will be removed to replace the primary equipment. All inventory controls and this document will be adjusted as needed.
SAMPLE DISASTER RECOVERY PLAN

Widget Department
Disaster Recovery Plan

Plan Objectives
In the event of a disaster, this Disaster Recovery Plan will be used by designated Information Technology staff to preserve important electronic data and physical IT resources from total loss. Disasters for the purposes of this plan are defined as:

1. Destruction or failure of hardware
2. Destruction or loss of facility resources
3. Destruction of data or loss of data integrity

This plan outlines the following essential tasks that IT staff must perform to recover from and minimize data/hardware loss in the event of a disaster:

- Maintenance of secondary hardware resources
- Data storage requirements
- Data backup techniques and frequency
- Access Control Management for temporary systems
- Coordination with the Business Continuity Planning team to execute this plan during a disaster

This Disaster Recovery Plan will be reviewed annually and revised as hardware/software and data needs change for Widget Department. The plan will be tested annually in coordination with the Business Continuity Plan testing as part of Widget Department’s Incident Response program testing.

IMPORTANT: All hardware/software and data retention plans for Widget Department MUST comply with the parent company’s policies, PCI DSS, PA DSS and any other regulatory body that governs how payment card transactions are processed.

Maintenance of Secondary Resources
Fail-over to the secondary location will be initiated for all disaster types. Daily maintenance of the secondary facility is automated; however, the Personnel Manager and IT Manager are required to visit the location at least monthly or if a disaster at the secondary facility occurs. IT staff are required to view audit logs for the secondary system, as well as the primary system, in accordance with industry regulation.

Only designated IT staff and the Widget department Personnel Manager are permitted in the secondary facility. Multi-layer facility entry controls are in place that allow 24/7 access to the secondary system if needed. Access to the facility is monitored via surveillance camera and system logs from an electronic door locking system.

Data Storage Requirements
All system data is stored locally on the servers. At the end of the fiscal year after financial reports are generated, data from the 7th year prior to the current year is sanitized and transferred to removal media to manage disk space. The encryption keys for that data are stored in the safety deposit box and the media stored in another location, other than the primary or secondary locations. The integrity of the media is tested annually by the IT manager and Accounting manager.
Data Backup Procedures
The Widget department performs two different methods of data backup to ensure that in the event of disaster that critical business data can be maintained. The virtualization software installed on all physical hosts has a sync option that permits IT staff to mirror data from one node to another in real-time. The mirror process does not disrupt system operation. If system data is corrupt and mirrored to the secondary node, the secondary node can be restored to a 24 hour old image from the offsite backup discussed below.

In addition to the virtual mirror backup, all VMs have a backup agent for OffSiteBackup.Com which encrypts and sends backup images to the OffSiteBackup.Com datacenter. Data from this backup can be restored to any physical machine using the local backup agent installation. Only Widget IT staff can execute this restore and decryption of data. This backup is performed nightly.

Access Control for Secondary System
Access Control for the secondary system is identical to the primary system. The Firewalls have the same capabilities and configuration. If a configuration change the primary firewall is made, IT staff save the configuration file and upload remotely to the secondary firewall. Procedures are in place to ensure that the secondary system is identical to the primary at all times.

Execution of Disaster Recovery Plan
In the event of a disaster that disrupts business operation at the primary location, IT staff will notify Accounting and Business Office staff to begin implementing business continuity procedures. IT staff will migrate systems to the secondary location and test viability prior to announcing the move to the secondary facility.