Version [0.0]

[Date]

Presented by: Michael Nelson

[company name]

[Company address]



Disaster Recovery Plan

[Document subtitle]

# Disaster Recovery Plan

Every School Network needs to incorporate a Disaster Recovery Plan into their Technology Administration Documentation. This is a basic template for schools and districts to follow should a disaster strike and mitigation steps need to be taken.

## Plan Overview

| DRP Team: |  |
| --- | --- |
| Team Leader: |  |
| Member 1: |  |
| Member 2: |  |

## Objective

State the overall objective of the plan. It should delineate district policy for technology disaster recovery and describe the process for recovering mission critical data and telecommunications. It should summarize the recommended procedures in the event of an emergency and be modified and re-assessed after each emergency to verify validity, continuity, structure and approach.

## Goals

Identify each goal to meet the above Objective.

### Goal 1: Notification

Who needs to be notified immediately upon the discovery of a disaster? The development of a phone/email/text tree is critical. Appendix A has a sample phone tree you can use to develop your district tree.

### Goal 2: Assessment

Who will perform the initial assessment? What form will that take? Identify the assessment team in Appendix B. You need to identify which services and/or equipment has failed and the impact the failure will have. Describe each type of disaster:

Data Disaster: This includes corruption or total loss of data due to a physical or virtual event. Identify which databases were corrupted, or what mission critical data will need to be restored.

Equipment Disaster: Describe each piece of equipment that was damaged in the disaster. Appendix C has mission critical equipment listed and all related information.

Network Disaster: This is a disruption of telecommunications or network connections. Describe the type and factor of failure. Again Appendix B lists all critical equipment.

### Goal 3: Communication

You will need to identify the steps, people, and companies that need to be notified immediately. Also identify the method each notification should include. For example, the telephone company might need to be notified immediately by cellphone about the damage or outage. Another example might be communication with district staff through district email or district phone tree about the outage.

### Goal 4: Mitigation

What steps need to be taken in order to mitigate the disaster? What kind of timeline? Will you need a phased approach to re-establishing the connection or restoring the data? Describe the steps you will need to have to mitigate the disruption, corruption, or loss of equipment.

### Action Step 1: Notification

What action steps need to be taken in order to meet goal 1 above? Set this onto your timeline. A sample timeline has been included here as Appendix D.

### Action step 2: Assessment

In Appendix E I’ve included assessment matrix charts that you can use to help with your assessment. Be sure to have a start and end date/time to get goal 2 accomplished.

### Action Step 3: Communication

Fully describe who what when and how goal 3 will be addressed above.

### Action Step 4: Mitigation

I’ve included in appendix B a template for a list of equipment and data that may need to be replaced or restored. Fully describe the action steps needed on a timeline in order to fully mitigate the impact of the disaster on your network.

## Backup Strategy

Every Disaster Plan should have a strong backup strategy policy in-line with your school or district board guidelines and state revised statutes.

### Retention Policy

There’s many laws and different policies that govern data retention. For example, in Arizona any email that refers to a student by first and last name should be retained indefinitely. Email that contains only student records should be retained for a period of 5 years. Knowing and understanding your specific requirements is important to the success of your DRP. Check with your human resources department, school auditors, and state IT websites for information on retention policies, backup strategies, and any other elements that may be required as a part of your DRP.

### Test Restoration

Most policies require monthly test restorations to ensure data integrity and process. When devising a Backup strategy, be sure to include test restorations

### Key District Departments with backup strategy:

Here are some key departments that will need a backup strategy depending on the state and board policies regarding their area. Determine if they need: A: Full mirror or duplication of current system or site. B: Onsite backup and data storage with term. C: Offsite backup and data storage with term

|  |  |
| --- | --- |
| **KEY BUSINESS PROCESS** | **BACKUP STRATEGY** |
| IT Operations |  |
| Tech Support - Hardware |  |
| Tech Support - Software |  |
| Facilities Management |  |
| Email |  |
| Purchasing |  |
| Disaster Recovery |  |
| Finance |  |
| Contracts Admin |  |
| Warehouse & Inventory |  |
| Product Sales |  |
| Maintenance Sales |  |
| Human Resources |  |
| Testing Fully Mirrored Recovery site - |  |
| Workshop Fully Mirrored Recovery site - |  |
| Call Center |  |
| Web Site |  |

## Risk Management

There are many potential disasters that could occur, from lightning strikes to a widespread data virus effecting core email and data systems. List all the possible types of disasters, their probability, Impact, a brief description of consequences, and what can be done to mitigate or remediate each threat.

You will need to prepare these for each building or location within your network if different threats exist for each.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Potential Disaster** | **Probability Rating** | **Impact Rating** | **Consequences** | **Remediation/Mitigation** |
| Example :Flood | 3 | 4 | All critical equipment is located on 1st Floor | All entrances to data rooms have flood proof doors. |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Probability: 1=Very High, 5=Very Low Impact: 1=Total destruction, 5=Minor annoyance

## Evaluation

Now that you have your plan prepared, you will need to test and evaluate different scenarios to make sure you understand the workflow and how this plan can be a key element in restoring connectivity or data as quickly as possible. Appendix F has some scenarios you can use to test your plan.

## Call Canyon Horizon LLC!

If you need assistance with any of the elements of this plan, or would like our assistance in the development of your DRP, give us a call! We can be reached at 888-504-5543 or [info@canyonhorizon.com](mailto:info@canyonhorizon.com)!

## Disaster Recovery Plan Signoff

All members who assisted in the preparation of this document should sign this form.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| Print First and Last Name | Title | Signature | Date |
|  |  |  |  |
| Print First and Last Name | Title | Signature | Date |
|  |  |  |  |
| Print First and Last Name | Title | Signature | Date |
|  |  |  |  |
| Print First and Last Name | Title | Signature | Date |
|  |  |  |  |
| Print First and Last Name | Title | Signature | Date |
|  |  |  |  |
| Print First and Last Name | Title | Signature | Date |
|  |  |  |  |
| Print First and Last Name | Title | Signature | Date |
|  |  |  |  |
| Partner (Printed Name) | Partner (Signature) |  | Date |
|  |  |  |  |
| Print First and Last Name | Title | Signature | Date |

## Appendix A: Phone Tree

# **Key Personnel Contact Info**

| **Name, Title** | **Contact Option** | **Contact Number** |
| --- | --- | --- |
|  | Work |  |
|  | Alternate |  |
|  | Mobile |  |
|  | Home |  |
|  | Email Address |  |
|  | Alternate Email |  |
|  |  |  |
|  | Work |  |
|  | Alternate |  |
|  | Mobile |  |
|  | Home |  |
|  | Email Address |  |
|  | Alternate Email |  |
|  |  |  |
|  | Work |  |
|  | Alternate |  |
|  | Mobile |  |
|  | Home |  |
|  | Email Address |  |
|  | Alternate Email |  |
|  |  |  |
|  | Work |  |
|  | Alternate |  |
|  | Mobile |  |
|  | Home |  |
|  | Email Address |  |
|  | Alternate Email |  |
|  |  |  |
|  | Work |  |
|  | Alternate |  |
|  | Mobile |  |
|  | Home |  |
|  | Email Address |  |

# **External Contacts**

| **Name, Title** | | **Contact Option** | | **Contact Number** |
| --- | --- | --- | --- | --- |
| **Landlord / Property Manager** | |  | |  |
| Account Number None | |  | |  |
|  | | Work | |  |
|  | | Mobile | |  |
|  | | Home | |  |
|  | | Email Address | |  |
|  | |  | |  |
| **Power Company** | |  | |  |
| Account Number | | Work | |  |
|  | | Mobile | |  |
|  | | Home | |  |
|  | | Email Address | |  |
|  | |  | |  |
| **Telecom Carrier 1** | |  | |  |
| Account Number | | Work | |  |
|  | | Mobile | |  |
|  | | Fax | |  |
|  | | Home | |  |
|  | | Email Address | |  |
|  | |  | |  |
| **Telecom Carrier 2** | |  | |  |
| Account Number | | Work | |  |
|  | | Mobile | |  |
|  | | Home | |  |
|  | | Email Address | |  |
|  | |  | |  |
| **Hardware Supplier 1** | |  | |  |
| Account Number | | Work | |  |
|  | | Mobile | |  |
|  | | Emergency Reporting | |  |
|  | | Email Address | |  |
|  | |  | |  |
| **Server Supplier 1** | |  | |  |
| Account Number. | | Work | |  |
|  | | Mobile | |  |
|  | | Fax | |  |
|  | | Email Address | |  |
|  | |  | |  |
| **Workstation Supplier 1** | |  |  | |
| Account Number | | Work |  | |
|  | | Mobile |  | |
|  | | Home |  | |
|  | | Email Address |  | |
|  | |  |  | |
| **Office Supplies 1** | |  |  | |
| Account Number C3095783 | | Work |  | |
|  | | Mobile |  | |
|  | | Home |  | |
|  | | Email Address |  | |
| **Insurance – Name** | |  |  | |
| Account Number | | Work |  | |
|  | | Mobile |  | |
|  | | Home |  | |
|  | | Email Address |  | |
|  | |  |  | |
| **Site Security –** | |  |  | |
| Account Number | | Work |  | |
|  | | Mobile |  | |
|  | | Home |  | |
|  | | Email Address |  | |
|  | |  |  | |
| **Off-Site Storage 1** | |  |  | |
| Account Number | | Work |  | |
|  | | Mobile |  | |
|  | | Home |  | |
|  | | Email Address |  | |
|  | |  |  | |
| **Off-Site Storage 2** | |  |  | |
| Account Number | | User ID |  | |
|  | | Password |  | |
|  | | Home |  | |
|  | | Email Address |  | |
|  | |  |  | |
| **HVAC –** |  | |  | |
| Account Number | Work | |  | |
|  | Mobile | |  | |
|  | Home | |  | |
|  | Email Address | |  | |
|  |  | |  | |
| **Power Generator –** |  | |  | |
| Account Number | Work | |  | |
|  | Mobile | |  | |
|  | Home | |  | |
|  | Email Address | |  | |
|  |  | |  | |
| **Other –** |  | |  | |
| Account Number | Work | |  | |
|  | Mobile | |  | |
|  | Home | |  | |
|  | Email Address | |  | |
|  |  | |  | |

## Appendix C: System Recovery Plan Templates

## Disaster Recovery Plan for <System Name>

|  |  |
| --- | --- |
| SYSTEM |  |

|  |  |
| --- | --- |
| OVERVIEW |  |
| Type of System: (Server/switch/router) | Location:  Server Model:  Operating System:  CPUs:  Memory:  Total Disk:  System Handle:  System Serial #:  DNS Entry:  IP Address:  Other: |
| HOT SITE SERVER | Provide details |
| APPLICATIONS  (Use bold for Hot Site) |  |
| ASSOCIATED SERVERS |  |

|  |  |
| --- | --- |
| KEY CONTACTS |  |
| Hardware Vendor | Provide details |
| System Owners | Provide details |
| Database Owner | Provide details |
| Application Owners | Provide details |
| Software Vendors | Provide details |
| Offsite Storage | Provide details |

|  |  |
| --- | --- |
| BACKUP STRATEGY FOR SYSTEM ONE |  |
| Daily | Provide details |
| Monthly | Provide details |
| Quarterly | Provide details |

|  |  |
| --- | --- |
| **SYSTEM ONE** **DISASTER RECOVERY PROCEDURE** |  |
| Scenario 1  Total Loss of Data | Provide details |
| Scenario 2  Total Loss of HW | Provide details |

**ADDENDUM**

|  |  |
| --- | --- |
| **CONTACTS** |  |
|  |  |
|  |  |
|  |  |
|  |  |

**File Systems <date>**

|  |  |
| --- | --- |
| **File System as of <date>**  Minimal file systems to be created and restored from backup:  <List> | **Filesystem kbytes Used Avail %used Mounted on**  <Provide details> |
| Other critical files to modify | <Provide details> |
| Necessary directories to create | <Provide details> |
| Critical files to restore | <Provide details> |
| Secondary files to restore | <Provide details> |
| Other files to restore | <Provide details> |

## Appendix D: Damage ASsessment Form

## Damage Assessment Form

|  |  |  |
| --- | --- | --- |
| **Key Business**  **Process Affected** | **Description Of Problem** | **Extent Of Damage** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Appendix C: Other Forms

## Disaster Recovery Event Recording Form

|  |
| --- |
| **Description of Disaster:** |
| **Commencement Date:** |
| **Date/Time DR Team Mobilized:** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Activities Undertaken by DR Team** | **Date and Time** | **Outcome** | **Follow-On Action Required** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| **Disaster Recovery Team's Work Completed:** <Date> |
| **Event Log Passed to Business Recovery Team:** <Date> |

## Mobilizing the Disaster Recovery Team Form

* Following an emergency requiring recovery of technology infrastructure assets, the disaster recovery team should be notified of the situation and placed on standby.
* The format shown below can be used for recording the activation of the DR team once the work of the damage assessment and emergency response teams has been completed.

|  |
| --- |
| **Description of Emergency:** |
| Date Occurred: |
| Date Work of Disaster Recovery Team Completed: |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name of Team Member** | **Contact Details** | **Contacted On (Time / Date)** | **By Whom** | **Response** | **Start Date Required** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Relevant Comments (e.g., Specific Instructions Issued) | | | | | |

## Communications Form

* It is very important during the disaster recovery and business recovery activities that all affected persons and organizations are kept properly informed.
* The information given to all parties must be accurate and timely.
* In particular, any estimate of the timing to return to normal working operations should be announced with care.
* It is also very important that only authorized personnel deal with media queries.

|  |  |  |  |
| --- | --- | --- | --- |
| Groups of Persons or Organizations Affected by Disruption | Persons Selected To Coordinate Communications  to Affected Persons / Organizations | | |
| Name | Position | Contact Details |
| Parents/Students |  |  |  |
| Management & Staff |  |  |  |
| Suppliers |  |  |  |
| Media |  |  |  |
| Stakeholders |  |  |  |
| Others |  |  |  |

Ref: http://searchdisasterrecovery.techtarget.com/feature/IT-disaster-recovery-DR-plan-template-A-free-download-and-guide