MERIDIA INTERACTIVE SOLUTIONS
1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

Photo Communications Corp. DBA Meridia Audience Response

CloudVOTE Disaster Recovery Plan

Last Update: 12/09/16

1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

Table of Contents

Information Technology Statement of Intent 4
Policy Statement 4
Objectives 4
Key Personnel Contact Info Emergency Response Team (ERT) 5
Notification Calling Tree 6
External Contacts 7
External Contacts Calling Tree 7
1 Plan Overview 8
1.1 Plan Updating 8
1.2 Plan Documentation Storage 8
1.3 Backup Strategy 8
1.4 Risk Management 9
2 Emergency Response 9
2.1 Alert, escalation and plan invocation 9
2.1.1 Plan Triggering Events 9
2.1.2 Activation of Emergency Response Team 9
2.2 Disaster Recovery Team 10
2.3 Emergency Alert, Escalation and DRP Activation 10
2.3.1 Emergency Alert 10
2.3.2 DR Procedures for Management 10
2.3.3 Contact with ERT 10
2.3.4 Backup Staff 10
2.3.5 Recorded Messages / Updates 11
2.3.7 Alternate Recovery Facilities / Hot Site 11
4 Insurance 11
5 Financial and Legal Issues 12
5.1 Financial Assessment 12
5.2 Financial Considerations 12
5.3 Legal Actions 12
6 DRP Exercising 12
Appendix A – Technology Disaster Recovery Plan 13
Disaster Recovery Plan for CloudVOTE Instance 13
Disaster Recovery Plan for CloudVOTE Instance 15
Disaster Recovery Plan for CloudVOTE Instance 17
Appendix B – Damage Assessment Form 19
Management of DR Activities Form 19

1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

Disaster Recovery Event Recording Form 20
Disaster Recovery Activity Report Form 21
Mobilizing the Disaster Recovery Team Form 21
Mobilizing the Business Recovery Team Form 22
Monitoring Business Recovery Task Progress Form 22
Preparing the Business Recovery Report Form 23
Communications Form 24
Returning Recovered Business Operations to Business Unit Leadership 24
Business Process/Function Recovery Completion Form 25

MERIDIA INTERACTIVE SOLUTIONS
1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

Information Technology Statement of Intent

This document delineates our policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms as they relate to Hosted CloudVOTE SaaS Product ("Service"). This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our people, our systems, and our data.

Our mission is to ensure personnel safety, information system uptime, data integrity and availability, and business continuity.

Policy Statement

Corporate management has approved the following policy statement:

- The company shall develop a comprehensive Service disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical hosted infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

Objectives

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the Service recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts the Service and dependent business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan.
- The need to ensure that operational policies are adhered to within all planned activities.
- The need to ensure that proposed contingency arrangements are cost-effective.
- The need to consider implications on all Service instances.
- Disaster recovery capabilities as applicable to key customers, vendors and others.

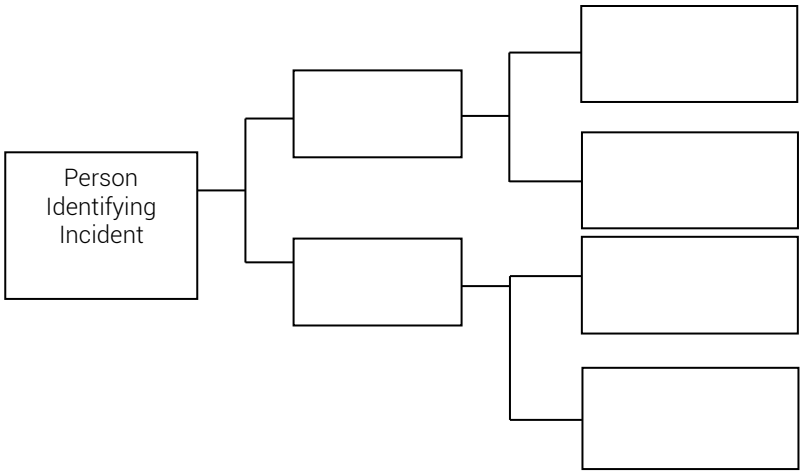
1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

Key Personnel Contact Info
Emergency Response Team (ERT)

Name, Title	Contact Option	Contact Number
	Business	
	Mobile	
	Primary	
	Alternate	
	Business	
	Mobile	
	Primary	
	Alternate	

1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

Notification Calling Tree

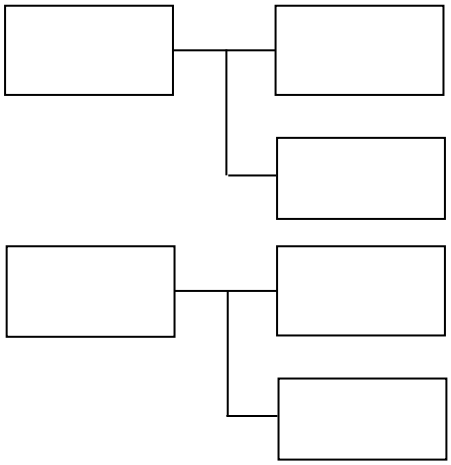


1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

External Contacts

Name, Title	Contact Option	Contact Number

External Contacts Calling Tree



1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

1 Plan Overview

1.1 Plan Updating

It is necessary for the DRP updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the training materials. This will involve the use of formalized change control procedures under the control of the COO.

1.2 Plan Documentation Storage

Copies of this Plan, CD, and hard copies will be stored in secure locations to be defined by the company. Each member of senior management will be issued a CD and hard copy of this plan to be filed at home. Each member of the Disaster Recovery Team and the Business Recovery Team will be issued a CD and hard copy of this plan. A master protected copy will be stored on specific resources established for this purpose.

1.3 Backup Strategy

Key CloudVOTE Components, agreed backup strategy, and primary and backup location for each are listed below. The strategy chosen is for a fully geo-redundant recovery site (either "West US", "East US" or "Central US"). This strategy entails the maintenance of a fully mirrored duplicate site, which will enable instantaneous switching between the live site (Primary) and the recovery (Backup) site.

KEY CLOUDVOTE COMPONENT	BACKUP STRATEGY (Primary/Backup)
Azure App Service	Fully mirrored recovery site (East US/West US)
Azure Storage	Fully mirrored recovery site (East US/West US)
Azure SQL Database	Fully mirrored recovery site (East US/West US)
Azure Cloud Service	Fully mirrored recovery site (East US/West US)

1.4 RISK MANAGEMENT

There are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section.

Potential disasters have been assessed as follows:

Potential Disaster	Probability Rating	Impact Rating	Potential Consequences	Brief Description Of Remedial Actions
Virus/Malware	3	2	Application malfunction	Anti-malware cleanup, automatic switch to backup site
Hack/Intrusion	3	2	Compromised security & privacy	Immediate shutdown and automatic switch to backup, follow-up code review
Environment failure	3	1		Automatic switch to backup
Regional failure	5	1		Automatic switch to backup

Probability: 1=Very High 5=Very Low

Impact: 1=Total destruction 5=Minor annoyance

2 Emergency Response

2.1 ALERT, ESCALATION AND PLAN INVOCATION

2.1.1 Plan Triggering Events

Key trigger issues at the live site that would lead to activation of the DRP are:

- Total loss of all communications
- Total loss of power
- Hack/Digital Intrusion
- Loss of the building

2.1.2 Activation of Emergency Response Team

When an incident occurs, the Emergency Response Team (ERT) must be activated. The ERT will then decide the extent to which the DRP must be invoked. All employees must be issued a Quick Reference card containing ERT contact details to be used in the event of a disaster. Responsibilities of the ERT are to:

- Respond immediately to a potential disaster and call emergency contacts;
- Allocate responsibilities and activities as required;
- Assess the extent of the disaster and its impact on business functions, application continuity, etc.;
- Decide which elements of the DR Plan should be activated;
- Establish and manage disaster recovery team to maintain vital services and return to normal operation.

2.2 Disaster Recovery Team

The team will be contacted and assembled by the ERT. The team's responsibilities include:

- Establish facilities for an emergency level of service within one (1) business hour;
- Restore key services within two (2) business hours of the incident;
- Recover to business as usual within eight (8) to twenty-four (24) hours after the incident;
- Coordinate activities with disaster recovery team;
- Report to the emergency response team.

2.3 Emergency Alert, Escalation and DRP Activation

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

2.3.1 Emergency Alert

The person discovering the incident calls a member of the Emergency Response Team in the order listed:

Emergency Response Team

- First Contact
- Second Contact
- Third Contact

If not available try:

- First Backup Contact
- Second Backup Contact

The Emergency Response Team (ERT) is responsible for activating the DRP for disasters identified in this plan, as well as in the event of any other occurrence that affects the company's capability to perform normally.

One of the tasks during the early stages of the emergency is to notify the Disaster Recovery Team (DRT) that an emergency has occurred. The notification will request DRT members to assess all available information about the problem and will involve sufficient details to have this request effectively communicated. The Business Recovery Team (BRT) will consist of senior representatives from the main business departments. The BRT Leader will be a senior member of the company's management team, and will be responsible for taking overall charge of the process and ensuring that the company returns to normal working operations as early as possible.

2.3.2 DR Procedures for Management

Members of the Meridia management team will keep a hard copy of the names and contact numbers of each member of the ERT. In addition, management team members will have a hard copy of the company's disaster recovery and business continuity plans on file in their homes in the event that the headquarters building is inaccessible, unusable, or destroyed.

2.3.3 Contact with ERT

Meridia managers will serve as the focal points in case of emergency, while designated contacts will notify the ERT, discuss the crisis/disaster and the company's immediate plans. If members of the Meridia management or others on ERT cannot reach one of the designated contacts, they are advised to call the secondary (emergency) contact to relay information on the disaster.

2.3.4 Backup Staff

If a Meridia manager or staff member designated to contact other members of the ERT is unavailable or incapacitated, the designated backup staff member will perform notification duties.

2.3.5 Recorded Messages / Updates

For the latest information on the disaster and the organization's response, ERT members can call any of the numbers listed in the DRP wallet card. Included in messages will be data on the nature of the disaster, steps taken toward recovery so far, and any updates on latest progress of work resumption.

2.3.7 Alternate Recovery Facilities / Hot Site

Automatically, through a geo-redundant failover mechanism, the hot site will be activated and notification will be given via email, phone or through communications with managers.

4 Insurance

As part of the Service disaster recovery and business continuity strategies a number of insurance policies have been put in place. These include errors and omissions, directors & officers liability, general liability, and business interruption insurance.

If insurance-related assistance is required following an emergency out of normal business hours, please contact:

Policy #	Coverage Type	Coverage Period	Amount Of Coverage	Next Renewal Date

5 Financial and Legal Issues

5.1 Financial Assessment

The emergency response team shall prepare an initial assessment of the impact of the incident on the financial affairs of the Service. The assessment should include:

- Loss of uptime
- Loss of information
- Extraneous cost related to employing emergency resources

5.2 Financial Considerations

The immediate financial consideration of/on the Service must be addressed. These can include:

- Immediate effect of downtime on Service revenue
- Temporary cost increase due to resiliency failover

5.3 Legal Actions

The company legal department and Meridia management will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event; in particular, the possibility of claims by or against the company for regulatory violations, etc.

6 DRP Exercising

Disaster recovery plan exercises are an essential part of the plan development process. In a DRP exercise, everyone who participates learns what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

Successful DR plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times. The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens.

1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

Appendix A – Technology Disaster Recovery Plan

DISASTER RECOVERY PLAN FOR CLOUDVOTE INSTANCE

SYSTEM	"CloudVOTE"

OVERVIEW	
PRODUCTION SERVER	Location: East US System Handle: CloudVotePollHub20 Resource Group: CloudVote2.0
HOT SITE SERVER	West US
APPLICATIONS	App Service (Website Login)
ASSOCIATED SERVERS	CloudVoteStorage20 CloudVoteSQL

KEY CONTACTS	
SYSTEM OWNERS	

BACKUP STRATEGY	
DAILY	Geo-Replicated to West US region
MONTHLY	External (Azure Storage) backup

DISASTER RECOVERY PROCEDURE	
SCENARIO 1 *TOTAL LOSS OF DATA*	Automatic, immediate switch to West US hot site
SCENARIO 2 *TOTAL LOSS OF HW*	Automatic, immediate switch to West US hot site

1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

ADDENDUM

CONTACTS	
PRIMARY	
SECONDARY	

File System as of 12/30/16	
USER ACCOUNTS	
NECESSARY ACCOUNTS TO CREATE	

1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

DISASTER RECOVERY PLAN FOR CLOUDVOTE INSTANCE

SYSTEM	"CloudVOTE"

OVERVIEW	
SERVER	Location: East US System Handle: CloudVoteSQL Resource Group: CloudVoteRedux
HOT SITE SERVER	West US
APPLICATIONS	SQL Database (session data)
ASSOCIATED SERVERS	CloudVoteStorage20 CloudVotePollHub20

KEY CONTACTS	
SYSTEM OWNERS	

BACKUP STRATEGY	
DAILY	Geo-Replicated to West US region
MONTHLY	External (Azure Storage) backup

DISASTER RECOVERY PROCEDURE	
SCENARIO 1 *TOTAL LOSS OF DATA*	Automatic, immediate switch to West US hot site
SCENARIO 2 *TOTAL LOSS OF HW*	Automatic, immediate switch to West US hot site

1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

ADDENDUM

CONTACTS	
PRIMARY	
SECONDARY	

File System as of 12/30/16	
USER ACCOUNTS	
NECESSARY DATABASE ENTRY TO RESTORE	

1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

DISASTER RECOVERY PLAN FOR CLOUDVOTE INSTANCE

SYSTEM	"CloudVOTE"

OVERVIEW	
EQUIPMENT	Location: East US System Handle: CloudVoteStorage20 Resource Group: CloudVote2.0
HOT SITE EQUIPMENT	West US
SPECIAL APPLICATIONS	Blob Storage (template data – images)
ASSOCIATED SERVERS	CloudVotePollHub20 CloudVoteSQL

KEY CONTACTS	
SYSTEM OWNERS	

BACKUP STRATEGY	
DAILY	Geo-Replicated to West US region
MONTHLY	External (Azure Storage) backup

DISASTER RECOVERY PROCEDURE	
SCENARIO 1 *TOTAL LOSS OF DATA*	Automatic, immediate switch to West US hot site
SCENARIO 2 *TOTAL LOSS OF HW*	Automatic, immediate switch to West US hot site

1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

ADDENDUM

CONTACTS	
PRIMARY	
SECONDARY	

File System as of 12/30/16	
USER ACCOUNTS	
NECESSARY TEMPLATES TO RESTORE	

1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

Appendix B – Damage Assessment Form

Key Business Process Affected	Description Of Problem	Extent Of Damage

Initials: _____

MANAGEMENT OF DR ACTIVITIES FORM

- During the disaster recovery process all activities will be determined using a standard structure;
- Where practical, this plan will need to be updated on a regular basis throughout the disaster recovery period;
- All actions that occur during this phase will need to be recorded.

Activity Name:
Reference Number:
Brief Description:

Commencement Date/Time	Completion Date/Time	Resources Involved	In Charge

Initials: _____

1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

DISASTER RECOVERY EVENT RECORDING FORM

- All key events that occur during the disaster recovery phase must be recorded.
- An event log shall be maintained by the disaster recovery team leader.
- This event log should be started at the commencement of the emergency and a copy of the log passed on to the business recovery team once the initial dangers have been controlled.
- The following event log should be completed by the disaster recovery team leader to record all key events during disaster recovery, until such time as responsibility is handed over to the business recovery team.

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:
Event Log Passed to Business Recovery Team:

Initials: _____

1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

Disaster Recovery Activity Report Form

- On completion of the initial disaster recovery response the DRT leader should prepare a report on the activities undertaken.
- The report should contain information on the emergency, who was notified and when, action taken by members of the DRT together with outcomes arising from those actions.
- The report will also contain an assessment of the impact to normal business operations.
- The report should be given to business recovery team leader, with a copy to senior management, as appropriate.
- A disaster recovery report will be prepared by the DRT leader on completion of the initial disaster recovery response.
- In addition to the business recovery team leader, the report will be distributed to senior management

The report will include:

- A description of the emergency or incident
- Those people notified of the emergency (including dates)
- Action taken by members of the DRT
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Assessment of the effectiveness of the BCP and lessons learned
- Lessons learned

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)					

Initials: _____

Mobilizing the Business Recovery Team Form

- Following an emergency requiring activation of the disaster recovery team, the business recovery team should be notified of the situation and placed on standby.
- The format shown below will be used for recording the activation of the business recovery team once the work of the disaster recovery team has been completed.

Description of Emergency:
Date Occurred:
Date Work of Business 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)					

Initials: _____

Monitoring Business Recovery Task Progress Form

- The progress of technology and business recovery tasks must be closely monitored during this period of time.
- Since difficulties experienced by one group could significantly affect other dependent tasks it is important to ensure that each task is adequately resourced and that the efforts required to restore normal business operations have not been underestimated.

Note: A priority sequence must be identified although, where possible, activities will be carried out simultaneously.

Recovery Tasks (*Order of Priority*)	Person(s) Responsible	Completion Date		Milestones Identified	Other Relevant Information
		Estimated	Actual		
1.					
2.					
3.					
4.					
5.					

Initials: _____

1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

Preparing the Business Recovery Report Form

- On completion of business recovery activities the BRT leader should prepare a report on the activities undertaken and completed.
- The report should contain information on the disruptive event, who was notified and when, action taken by members of the BRT together with outcomes arising from those actions.
- The report will also contain an assessment of the impact to normal business operations.
- The report should be distributed to senior management, as appropriate.

The contents of the report shall include:

- A description of the incident
- People notified of the emergency (including dates)
- Action taken by the business recovery team
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Problems identified
- Suggestions for enhancing the disaster recovery and/or business continuity plan
- Lessons learned

1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

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.

Groups of Persons or Organizations Affected by Disruption	Persons Selected To Coordinate Communications to Affected Persons / Organizations		
	Name	Position	Contact Details
Customers			
Management & Staff			
Stakeholders			
Others			

Initials: _____

Returning Recovered Business Operations to Business Unit Leadership

- Once normal business operations have been restored it will be necessary to return the responsibility for specific operations to the appropriate business unit leader.
- This process should be formalized in order to ensure that all parties understand the change in overall responsibility, and the transition to business-as-usual.
- It is likely that during the recovery process, overall responsibility may have been assigned to the business recovery process lead.
- It is assumed that business unit management will be fully involved throughout the recovery, but in order for the recovery process to be fully effective, overall responsibility during the recovery period should probably be with a business recovery process team.

1646 West Chester Pike, Suite 15, West Chester, PA 19382
Phone: 610-260-6800, Fax: 610-260-6810, Email: rsvp@meridiaars.com

Business Process/Function Recovery Completion Form

The following transition form should be completed and signed by the business recovery team leader and the responsible business unit leader, for each process recovered.

A separate form should be used for each recovered business process.

Name Of Business Process	
Completion Date of Work Provided by Business Recovery Team	
Date of Transition Back to Business Unit Management *(If different than completion date)*	

I confirm that the work of the business recovery team has been completed in accordance with the disaster recovery plan for the above process, and that normal business operations have been effectively restored.

Business Recovery Team Leader Name: _____

Signature: _____

Date: _____

(Any relevant comments by the BRT leader in connection with the return of this business process should be made here.)

I confirm that above business process is now acceptable for normal working conditions.

Name: _____

Title: _____

Signature: _____

Date: _____