Business Continuity

Client Briefing

About this document

This document describes Mediaocean's disaster recovery and business continuity policy.

T +1 212 633 8100
INFO@MEDIAOCEAN.COM
MEDIAOCEAN.COM

mediaocean

TABLE OF CONTENTS

T +1 212 633 8100
INFO@MEDIAOCEAN.COM
MEDIAOCEAN.COM

Policy

Company mission statement

Mediaocean is the world's only software company that automates every aspect of the advertising workflow, from planning and buying, to analyzing and optimizing, to invoicing and payments. Its open platforms have unmatched reach and bridge traditional and digital media, serving more than 80,000 users across agencies and brands worldwide and powering $100 billion in global media buying.

Mediaocean's mission is to build open, intuitive, universal enterprise software solutions for the global advertising community by:

- Creating software that leads advertising into the future
- Developing systems that make global advertising efficient, reliable and limitless
- Offering the advertising world complete access to the best data, relevant media, and emerging technologies
- Becoming the global standard for unifying data, optimizing workflow, and delivering intelligence
- Developing applications whose design and usability make workflow seamless and easy
- Delivering systems the advertising world will count on most

IT mission statement

As an application service provider, Mediaocean relies on its computer and communication resources to support many essential business processes for our clients. IT's mission is to ensure the availability of these resources in accordance with defined service level agreements and performance standards, while maintaining the integrity and confidentiality of data processed via these resources.

Objectives

The objective of Mediaocean's Business Continuity Plan (BCP) is to support the company's mission by ensuring that critical business processes can be continued in the event of a declared disaster and to provide the framework to re-establish normal operations within the shortest possible time frame.

The BCP aims to ensure that in the event of a declared disaster:

- Client access to Mediaocean transactional systems and essential support services is restored within 12 hours of invocation via a detailed prioritized and timetabled response
- Reporting is restored within 24 hours of invocation.
- Communications with stakeholders are managed effectively
- Staff welfare and confidence are maintained
- Expenditure is controlled and extraordinary costs are minimized.

Key personnel will be trained and prepared to respond to a disaster, and execute effective recovery actions to restore critical business operations.

Scope

This policy applies to all Mediaocean offices and staff, and to the following Mediaocean applications:

Application/suite	Hosted at	Backed up at
North America		
Aura	**IBM Sterling Forest** Data Center, NY	**Mediaocean London** Data Center, UK
Connect	**IBM Sterling Forest** Data Center, NY	**Mediaocean London** Data Center, UK
Invision DealMaker / DMD CrossRoad / Propost	**QTS** Data Center, GA	**Equinix** Data Center, New Jersey
Lumina / MMP	**AWS** Cloud Service	**AWS** Cloud Service
Prisma / Prisma for Sellers	**IBM Sterling Forest** Data Center, NY	**Mediaocean London** Data Center, UK
Spectra AV	**Mediaocean Louisville** Data Center, KY	**CenturyLink Elk Grove** Data Center, IL
Spectra DS	**IBM Sterling Forest** Data Center, NY	**Mediaocean London** Data Center, UK
Spectra OX	**CenturyLink Elk Grove** Data Center, IL	**Mediaocean Louisville** Data Center, KY
Australia / Pacific		
Ignitia	**AWS** Cloud Service	**AWS** Cloud Service
MScope	**Self hosted** by clients	Responsibility of clients
Spectra MD	**Self hosted** by clients, or at **Mediaocean Sydney** Data Center, AUS	Responsibility of clients**,** or **Mediaocean Melbourne** Data Center, AUS
Spectra PF	**Self hosted** by clients, or at **Mediaocean Sydney** Data Center, AUS	Responsibility of clients**,** or **Mediaocean Melbourne** Data Center, AUS
Europe Aura	 **IBM Sterling Forest** Data Center, NY	 **Mediaocean London** Data Center, UK
Lumina	**AWS** Cloud Service	**AWS** Cloud Service
Prisma / PATS	**IBM Sterling Forest** Data Center, NY	**Mediaocean London** Data Center, UK
Spectra AS	**Self hosted** by clients	**Self hosted** by clients
Spectra DS	**IBM Sterling Forest** Data Center, NY	**Mediaocean London** Data Center, UK
Spectra MX	**IBM Sterling Forest** Data Center, NY	**Mediaocean London** Data Center, UK

Key requirements

1. Staff clearly understand how incidents in Mediaocean's different locations affect systems and services, both client facing and internally
2. Potential risks within Mediaocean's processing environment are identified and mitigated where it is cost effective to do so. Risk avoidance is a critical element in the Disaster/Business recovery process.
3. Decision making and tactical roles are clearly defined, with established ownership for the recovery process and assigned responsibilities to assess, escalate, and declare a disaster
4. Effective data retention practices (including data mirroring and off-site storage) and prioritized technical recovery plans are documented, reviewed and tested regularly
5. External communications to clients and partners are based on management briefings
6. Procedures for internal communications to staff and contractors are clearly defined, including expected timing and frequency of communications
7. Staff clearly understand their personal recovery and continuity responsibilities, including being aware of their local office's safety and evacuation procedures.

Responsibilities

This policy is owned by the Information Security Director, Jeffrey Aschenbach.

Crisis Management Team

The Crisis Management Team (CMT) is the decision making group who will be responsible for deciding, based on recommendations from the Incident Response Team, whether to declare a disaster and invoke the BCP.

This team is responsible for overseeing business continuity planning, and for ensuring that adequate resources are provided to execute it.

In the event that the CMT declares a disaster, the team is responsible for authorizing internal and external communications plans, and for approving extraordinary costs associated with the incident. The team approves facilities renovation and reconstruction activities and takes decisions about when the company is ready to resume normal business operations following an incident.

Following an incident, the CMT assesses the performance of the teams involved in recovery and the overall effectiveness of the BCP.

Incident Response Team

The Incident Response Team (IRT) is a group of senior managers with overall responsibility for their team's recovery and continuity planning, and for educating staff on disaster notification and recovery procedures.

In the event of an incident the IRT is responsible for assembling and briefing a damage assessment team. Based on this team's findings, the IRT will recommend the declaration of a disaster to the CMT if appropriate, and prepare internal and external briefings for approval by the CMT. The IRT liaises with the tactical team to oversee progress of the recovery. The IRT is also responsible for invoking recovery at fail-over sites where applicable.

Following an incident, the IRT is responsible for reporting performance of recovery teams and overall effectiveness of recovery and continuity plans to the CMT.

Tactical Team

The Tactical Team is a group of managers in each location who execute / manage specific recovery tasks once the IRT has agreed to invoke the recovery plan.

Line managers

All line managers will play a key role in passing on communications from the IRT to the rest of the company, and, if required, for ensuring that all staff are safely accounted for. For this reason, **all line managers must make sure that their mobile phones are used to store the mobile and/or home numbers of all their direct reports**, as well as the numbers of their line manager and of any other managers they will need to work with closely in executing the recovery plan.

Line managers are also responsible for ensuring that their direct reports understand their specific responsibilities for executing the recovery plan.

All staff

All staff are responsible for ensuring they understand their role in the recovery plan and must check with their line manager if they are not sure.

All staff must familiarize themselves with their office's safety precautions and evacuation procedures. All staff must store their line manager's phone number in their mobile phone.

Staff in the following departments have the following specific responsibilities:

Department	Responsibility
Development	During disaster: Provide programming support as needed to solve any code related problems during the move to the back-up site, during restoration procedures or during reinstallation at the permanent location
IT Operations	Prior to disaster: Document and maintain procedures for the restoration of Mediaocean's applications, databases, network and communications configurations in the event of a disaster; provide specifications for back-up sites; where Mediaocean data centers are functioning as back-up sites for other data centers, provide an environment adequate to restore critical information systems and communication services to the client base During disaster: Work to ensure that services may be delivered to the client base from the back-up site After disaster: Reintroduce normal processing from the permanent facility as soon as it is available and reestablish the required data, equipment and communications
Client Service	Prior to disaster: Maintain an up to date listing of key client contacts to be contacted in the event of a disaster. Listing to include Mediaocean owner of the client contact During disaster: Ensure that all appropriate key client contacts and users are notified of the disaster and the anticipated timetable of recovery; provide updates as prescribed by Mediaocean procedures and/or client SLAs; Provide application support from the alternative site or remotely After disaster: Ensure that all appropriate key client contacts and users are notified that recovery is complete and system is operational; provide application support and internal escalation for any issues reported due invoking DR
HR / Finance	During disaster: Provide for the well-being of personnel; Arrange for expenses and payment of invoices

Assumptions

In the process of developing a Business Continuity Plan (BCP), assumptions often have to be made, e.g., the Recovery Location is available at the time of disaster, designated backup staff is available, etc. The following assumptions were made when generating this plan:

- **Personnel Safety -** In all situations, the safety of all people is the first priority.
- **Focus is on a local disaster -** The BCP's primary focus is on a local worst-case interruption to any of the Mediaocean sites (for example, earthquake, fire, power outage, flood, or sabotage; that is, all equipment, electronic files, procedures and documentation, and the data center are not usable). A worst case disaster can result in a long-term outage, perhaps as long as six to eight weeks, or more. The mean time to repair/replace a data center in this event dictates the need for an alternate computer site, or "back-up site", along with communications network back-up strategies.
- **Key personnel -** This BCP requires that key technical personnel with specific skills (including HP, Oracle, mainframe, LAN and WAN) are available during a disaster for the recovery process to be successful. This includes primary and/or backup personnel. If key personnel are not available, the skills will be obtained from other Mediaocean or IT Organization locations and vendors.
- **Staff awareness and understanding –** this BCP requires that all Mediaocean staff have been trained and made aware of their business continuity and recovery responsibilities. Reference documentation to support staff understanding and knowledge of these procedures is made available off-site, both via a back-up Alfresco server and via hard copies distributed to key individuals.
- **Data storage -** Mediaocean currently subscribes to various data retention strategies, including data mirroring and off-site storage. Mediaocean has appointed different secure storage vendors in different locations for storage services. It is assumed that full system backups (production application and operating system files; transaction logs and/or data base image tapes) will be done on a scheduled basis and will be rotated to off-site storage on an adequate basis to meet the requirements of the business functions.
- **Individual support procedures -** The IT Operations group is responsible for the coordination of all recovery support procedures such as network and systems support. However, it is the responsibility of each support area to ensure the procedures are documented, maintained, and provided to the IT Operations group.
- **Testing the plan -** Testing of this BCP will be performed annually. Mediaocean management and IT Operations Team will jointly agree on the scope of the test.
- **Response time at recovery site -** In a disaster, Mediaocean is relieved of its obligation to meet performance standards in any SLA; however Mediaocean will attempt to re-establish normal operations after the Critical Business Applications (CBAs) are stable.
- **Ability to meet defined RTO –** Mediaocean's RTOs have been agreed taking into account both business needs and technical capabilities in order to define a realistic timescale for recovery of CBAs and services to clients.
- **Recovery point objectives (RPO) and acceptable data loss** – for all application suites except Lumina and Invision, data mirroring has been implemented at data centers to copy data continually to a secondary data center to reflect the fact that Mediaocean's acceptable data loss is limited to less than 20 minutes. This is achieved by configuring database replications to take place at least every 15 minutes. For Lumina MMP, the current RPO is 4 hours. For Invision, the client specifies their selected recovery point objective in their Service Level Agreement.

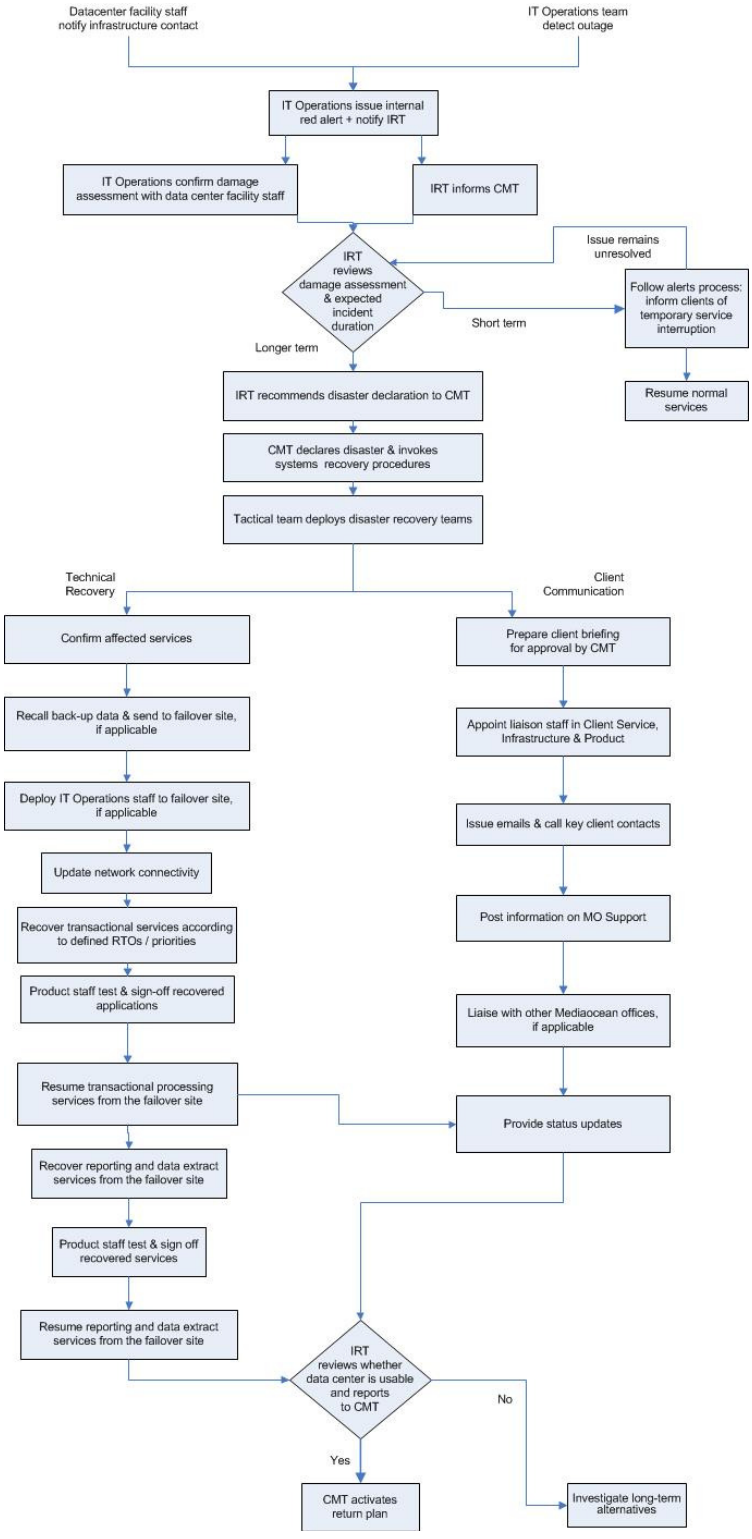
Overview

The table below identifies, for each Mediaocean location, what systems are running and the impact of an incident in that location.

Site	Systems	Users affected	Recovery strategy
Data centers			
AWS Cloud Service	Lumina / MMP Ignitia	Lumina, MMP and Ignitia users	AWS contract provides for resilience services Alternatively, restore from offsite backup tapes at a Mediaocean data center
CenturyLink Elk Grove, IL	Spectra OX Email (Outlook / Exchange) Skype for Business Replicated back-ups for Spectra AV	Spectra OX users in North America All Mediaocean staff will lose email access	Recover systems and office services at Louisville using data replicated to Louisville Email services to fail over to Louisville
IBM Sterling Forest, NY	Aura, Optica, Spectra DS and Prisma MO Support library Alfresco / Confluence / Skype for Business Intranet / JIRA / Lotus Notes 3CX phone system for Mediaocean North American offices	Aura, Optica, Spectra DS and Prisma clients worldwide MO Support users worldwide – for access to MO documentation only	Client facing applications to fail over to the London back-up data center 3CX phone system and Skype for Business to fail over to CenturyLink Elk Grove Confluence / Alfresco: use back-up sites in London / Louisville JIRA / intranet / Notes: await recovery in London
QTS, GA	Invision systems: DealMaker, CrossRoad, DMD, Propost	Invision system users in North America	Recover systems at Equinix data center, Secaucus NJ using data replicated to Equinix
Mediaocean offices			
London	Replicated back-ups for Aura, Optica, Spectra DS and Prisma Local phone system In-office access to email and network services and to Spectra AS support systems Local development and QA environments	London users requesting printed reports Mediaocean staff based in London office Mediaocean staff with remote connections to London office	Recover office and printing services and Spectra AS systems at SunGard using local back-up data at Abbot Datastore Invoke alternative back-up strategy for Sterling Forest data center
Louisville	Spectra AV In-office access to email & network services Local development and QA environments Replicated back-ups for Spectra OX	Spectra AV users in North America Mediaocean staff based in Louisville office Mediaocean staff with remote connections to Louisville office	Recover systems and office services at CenturyLink Elk Grove using data replicated to CenturyLink.
Melbourne	Local network, phone system Security and domain services Local Development, UAT and QA environments	Mediaocean APAC staff in Melbourne office	Recover critical systems from replicated backups in Sydney office and allow staff to work from home

Site	Systems	Users affected	Recovery strategy
Sydney	Local network, phone system Security and domain services, Internal Spectra PF, Service Desk Client connections and VPNs Local Development, UAT and QA environments.	Mediaocean APAC staff in Sydney office Mediaocean APAC staff in Melbourne office Spectra MD and PF users who have opted to have Mediaocean host their services	Recover critical systems from replicated backups in Melbourne office and allow staff to work from home
All other offices	In-office access to email & network services Local development and QA environments	Mediaocean staff based in that office Mediaocean staff with remote connections to that office	Recover office services at locally defined recovery sites or allow staff to work from home

Recovery workflow – US data centers



Declaring a disaster

A disaster is defined as any catastrophic failure, including but not limited to, force majeure [1]events such as flood or earthquake, power loss, internet connectivity loss, major hardware or software failure, malicious attack, that threatens to render a Mediaocean office or data center inoperable for more than a twenty four (24) hour period without an imminent indication of recovery, resulting in Mediaocean either being unable to provide computer services to its clients, or being unable to provide email, web and phone support services to its clients.

Any individual who notices or is informed of a problem with a data center, network, or office location which may be a disaster must follow documented internal alert procedures.

The IRT is responsible for recommending to the CMT that a disaster should be declared. The CMT is then responsible for declaring the disaster. A disaster will be declared and the BCP invoked immediately when it is determined that critical services will be unavailable beyond the established critical point. The following activities will occur:

1. Mediaocean will initiate an alert for the affected system / network location as per the internal alert procedure. The alert will be issued via email if possible or alternatively by phone call. A senior member of the IT Operations team will then notify the IRT by phone (see Key Contacts document).
2. The IRT will ask IT Operations and building facilities staff as appropriate to conduct an assessment of the damage.
3. The IRT will review the results of the assessment and then determine if a disaster declaration should be made. A disaster will normally be declared if the assessment concludes that the damage to Information Systems equipment, the facility or the communications network is severe enough to prevent Mediaocean from providing critical business functions contracted by the client base for a period exceeding 24 hours within a Monday - Friday time frame.
4. The IRT will prepare a staff briefing for approval by the CMT about the disaster and, if out of office hours, will initiate disaster notification procedures, advising staff whether to report to work the next day and specifying time and location, if other than the normal office.
5. The CMT will authorize the Incident Management Team to invoke recovery at the back-up site.

The IRT may also meet to discuss a potential or impending disaster (such as severe weather) and perform a risk assessment which takes into account the potential harm which could be caused and the likelihood of the disaster occurring. The CMT may therefore decide to declare a disaster before the incident has actually taken place.

[1] A Force Majeure Event is defined as a fire, flood, earthquake, other elements of nature or acts of God, acts of war, terrorism, riots, rebellions or revolutions, civil disorders or third party labor strikes or disputes. Force Majeure events are beyond the control of Mediaocean and are likely to affect Mediaocean's ability to transfer services to the back-up data center. Force Majeure events have special provision in Mediaocean's standard Service Level Agreements so it is important that when a disaster is declared the Incident Response Team should identify whether or not Force Majeure applies and notify the clients accordingly.

Test Plan

This BCP is rehearsed regularly in order to validate Mediaocean's ability to resume and continue critical business processes in the event of a disaster. Testing the BCP provides the opportunity to train the personnel who are responsible for executing the Plan. The important idea is not that the test succeeds without problems, but that the test results and problems encountered are reviewed and used to update or revise the current procedures and plans.

Periodic testing validates the effectiveness of the backup and recovery procedures and confirms that documented recovery procedures are executable and accurate. It is expected that Mediaocean's system and network environment will change regularly; therefore, the BCP is tested annually to ensure that Mediaocean's most critical applications are available to support business in the event of a disaster. Standard test plan templates are documented for each production application to be recovered, and for office recovery tests. For each test to be conducted, the following elements are specified so the participants are well prepared and productive during the actual test:

- test parameters
- objectives
- measurement criteria
- task charts
- time lines

After each test has been conducted an evaluation of the test is performed to ensure that lessons are learned and follow-up actions are identified and implemented as necessary.

A formal test plan is documented for all production applications recovery tests and for office recovery testing, where applicable.

Test Procedure

Prior to the test

- Review what systems and applications are new or significantly changed since last test and confirm test goals
- Confirm test participants
- Agree test dates and book them with third parties where applicable

Set up test environment

- Arrange for transfer of back-up media if applicable
- Configure applications for test
- Configure VPCs as required
- Log any issues with set-up

Execute test procedures

- Document test results
- Report, fix and retest issues
- Monitor progress

After the test

- Dismantle test environment and ensure any data or software copied onto third party equipment has been securely removed
- Return back-up media to off-site storage if applicable
- Review test results
- Update recovery plans as appropriate

Maintenance plan

This BCP may be updated either as a result of annual review, or because of an event such as:

- Changes in operating system(s) or utility software programs
- Changes in the design of a production application database
- Changes in the data communication network design
- New application systems developed or purchased
- Discontinuance of an application system
- Transfers, promotions, and terminations of personnel

Annual Verification of the Business Continuity Plan

Annual verifications of the BCP should include:

- SLA Review
- Vital Records Audit
- Walk through and review by the IRT
- Business Impact Analysis Validation with Mediaocean IT Organizations.
- Review and validation of key staff and vendor contact lists

Recovery Procedures are validated and reviewed during the annual Test procedure.

Distribution and storage of the Business Continuity Plan

After annual verification of the BCP as described above, admin staff will mail an information pack to the home address of members of the IRT and Tactical Team members. This will contain key contact numbers, wallet cards, and workflow diagrams. The electronic version of this plan is located on the Mediaocean content management system.