ChildsPlay
Systems Ltd

Disaster Recovery Plan

Issued by:	**Ian Foster**
Version:	1.2, 1.3
Date:	03/08/2009, 19/05/2018
Copy Number:	C1 C2 C3

ChildsPlay Systems Ltd, Confidential

Table of Contents

1 Plan Revision History.
2 About This Disaster Recovery Plan.
3 Plan Objectives.
4 Disaster Management Team and Responsibilities.
5 What to do in the Event of a Disaster.
6 Recovery Scenarios.
7 The Standby Facilities.
8 The Data Storage Location
9 Critical Business Lessons
10 Directories
11 Inventories

1 Plan Revision History

It is important that this Disaster recovery Plan accurately reflects the current situation and business requirements at ChildsPlay Systems Ltd. Updates must be provided to Ian Foster.

The following table describes the history of this document.

Version	Date Issued	Reason for Update
1.0	12/03/2009	
1.1	20/04/2011	
1.2	19/05/2018	New GDPR Regulations

2. About This Disaster Recovery Plan

2.1.Purpose and Scope of This Plan

This plan has been designed and written to be used in the event of a disaster affecting ChildsPlay Systems Ltd at Innovation Centre Medway, Maidstone Rd, Chatham, Kent, ME5 9FD.

The decision to initiate disaster recovery procedures will be taken by the *Disaster Management Team Leader* or his deputy after assessing the situation following a disaster or crisis.

If the *Disaster Management Team Leader* decides to initiate disaster recovery procedures, then all members of the recovery teams will follow the procedures contained in this plan until recovery is complete.

This plan contains all the information necessary to restore an operational service in the event of a serious disruption of computer services at Innovation Centre Medway, Maidstone Rd, Chatham, Kent, ME5 9FD which will be called Company Offices for this plan.

2.2. Updating This Plan

This plan must be kept up to date.

It is the responsibility of **Adele Fincham** to ensure that procedures are in place to keep this plan up to date. If, whilst using the plan, you find any information which is incorrect, missing or if you have a problem in understanding any part of this plan please inform **Adele Fincham** so that it may be corrected. *It is important that everyone understands their role as described in this plan*.

Updated versions of the plan are distributed to the authorised recipients, listed in Section 2.3, Distribution List.

2.3. Distribution List

Ian Foster is responsible for distributing this plan. Each plan holder, listed in the table below, receives two copies of this plan. One copy is to be kept at the place of work and the other copy at home or other safe offsite location. These copies have an official copy number.

Each team leader must ensure that each team member has two copies of the plan.

Name	Copy Number
Adele Fincham	C3
Adam Gibson	C3
Ian Foster	C3

3. Plan Objectives

A disaster is defined as an incident which results in the loss of computer processing at the ChildsPlay Systems Ltd site at Company Offices, to the extent that relocation to a Standby Facility must be considered. A disaster can result from a number of accidental, malicious or environmental events such as fire, flood, terrorist attack, human error, software or hardware failures.

The primary objective of this Disaster recovery Plan is to ensure the continued operation of identified business critical systems in the event of a disaster.

Specific goals of the plan are:

- To try and maintain operational status at the Company Offices.
- To operate from standby facilities within <1> working days.
- To operate at the standby facility for up to 1 month.
- To reinstate ChildsPlay Systems Ltd facilities in the ChildsPlay Systems Ltd premises within the maximum working standby period
- To minimize the disruption to ChildsPlay Systems Ltd' as a business

4. Disaster Management Team and Responsibilities

This section defines the functional responsibilities of each recovery team.

The names of all the team members are to be listed in Section 10.2.1, Recovery Team Members.

4.1. Disaster Management Team

The Disaster Management Team is responsible for providing overall direction of the data centre recovery operations. It ascertains the extent of the damage, activates the recovery organisation and notifies the team leaders. Its prime role is to monitor and direct the recovery effort. It has a dual structure in that its members include Team Leaders of other teams.

The *Disaster Management Team Leader* is responsible for deciding whether or not the situation warrants the introduction of disaster recovery procedures. If he decides that it does, then the organisation defined in this section comes into force and, for the duration of the disaster, supersedes any current management structures.

The Disaster Management Team operates from the Command Centre.

4.1.1. Disaster Management Team Charter

The Disaster Management Team is responsible for the following:

- Making decisions about restoring the computer processing environment in order to provide the identified level of operational service to users.
- Managing all the recovery teams and liaising with ChildsPlay Systems Ltd's management, company headquarters and users, as appropriate.
- Maintaining audit and security control during the recovery from disaster.
- Controlling and recording emergency costs and expenditure.

4.1.2. Responsibilities

- Evaluating the extent of the problem and potential consequences.
- Notifying the staff of the disaster, recovery progress and problems.
- Initiating disaster recovery procedures.

- Co-ordinate recovery operations
- Monitoring recovery operations and ensuring that the schedule is met.
- Documenting recovery operations.
- Liaising with user management.
- Recording emergency extraordinary costs and expenditure.
- Making a detailed accounting of the damage to aid in insurance claims.
- Ensuring that the conversion to the standby facilities and the final resumption of operations at the data centre are under sufficient audit control to provide reliability and consistency to the accounting records.
- Monitoring computer security standards.
- Ensuring that appropriate arrangements are made to restore the site and return to the status quo within the time limits allowed for emergency mode processing.
- Approving the results of audit tests on the applications which are processed at the standby facility shortly after they have been produced.
- Performing a detailed audit review of the critical accounting files after the first back up cycle has been completed.
- Declaring that the Disaster recovery Plan is no longer in effect when computer processing is restored at the primary site.

5. What To Do in the Event of a Disaster

The most critical and complex part of the management of resources is in the planning and organisation of the required personnel during the invocation of the plan.

Personnel must be well-rehearsed, familiar with the Disaster recovery Plan and be sure of their assignments.

5.1. Standard Emergency Procedures

The first priority in a disaster situation is to ensure safe evacuation of all personnel.

In the event of a major physical disruption, standard emergency procedures must be followed. This means immediately:

- Activating the standard alarm procedures for that section of the building to ensure that Medical, Security and Safety departments and emergency authorities are correctly alerted.
- If necessary, evacuating the premises following the laid down evacuation procedures and assemble outside at the designated location, if it is safe to do so.
- Follow Emergency Action Plan see in ***Appendix 1***

5.2. The First Steps for the Recovery Teams

- The Disaster Team assesses the nature and extent of the problem.
- If it is safe to do so, the Disaster Team switches off all equipment in the building.
- The Disaster Team will make an initial assessment, as they need to know the extent of the damage to the buildings and equipment and the staff status. Also report what actions have been taken.

5.3. The Next Steps

The *Disaster Management Team Leader* decides whether to activate the Disaster recovery Plan, and which recovery scenario will be followed.

6. Recovery Scenarios

This section describes the various recovery scenarios that can be implemented, depending on the nature of the disaster and the extent of the damage. The *Disaster Management Team Leader* decides which recovery scenario to implement when he or she activates the Disaster recovery Plan.

6.1. Scenario One: Minor Damage

In this scenario, only a part of the computer processing environment is out of action, but the communication lines and network are still up and running. The goal of the recovery process in this case is to move the applications from the systems which are unavailable and replace them.

In this scenario the building is still available and the users can use normal office space to wait for the restart of damaged computers.

6.1.1. Action Plan

Task	**Team**
Evaluate the damage	Disaster
Identify the concerned applications	Disaster
Obtain the appropriate backups	Disaster
Inform users of the new procedures	Disaster
Order replacement equipment to replace the damaged computers.	Disaster

Install replacement equipment and restart the applications	Disaster

6.2. Scenario two: Communications/internet Damage

In this scenario, only a part of the computer processing environment is out of action, network are still up and running but communication lines are down. Call the telephone provider to establish what has happened and to plan next move.

6.2.1. Action Plan

Call the telephone provider or internet provider to establish what has happened and to plan next move. If the telephones off temporary then wait. If the lines will be down and will be for some time before coming backup then we go to facilities location and send customer emails from that location. At the same time one of the IT team will also go to a facilities location and change Website so that visitors and customers will be aware that we are unable to be contacted on normal lines and provide additional numbers to which we can be contacted on.

Task	**Team**
Evaluate the damage	Disaster
Contact suppliers	Disaster
Inform staff of the new procedures	Disaster
Inform customers from facilities location what has happened.	Disaster
Change website to state situation	Disaster

6.3. Scenario three: Building Damage

In this scenario, building/office in which the staff works is out of action.

6.3.1. Action Plan

Call all staff and make them aware of what has happened and arrange for them all to work from their facility locations. During this time key staff will email all customer of the situation and change the website. The website and the emails will have alternative contact numbers. If needed we will call all customers direct to make sure business can continue functioning. As our backups are held off site it will be straight forward for us to continue trading.

Task	Team
Evaluate the damage	Disaster
Contact suppliers	Disaster
Inform staff of the new procedures	Disaster
Inform customers from facilities location what has happened.	Disaster
Change website to state situation	Disaster
Access offsite backup data to continue trading.	Disaster

7. The Standby Facility

This section provides a general introduction to the standby facilities which the ChildsPlay Systems Ltd can utilise for computer processing <and office space> following a disaster. If the disaster is expected to take a long time then all staff will be asked to attend key location.

7.1. Location of the Standby Facility

The address of the Standby Facility is: Staff addresses

8. The Data Storage Location(s)

This section describes the location(s) of the vault facilities where secure copies of data backups and other vital information are stored.

8.1. Storage Location 1

Location and address:	
Contact person:	
Contact phone number:	
Type of device	
Type of safe:	
Maximum capacity:	
Content:	

9. Critical Business Lessons.

This section describes the system requirements for ChildsPlay Systems Ltd critical business applications in the standby facility.

It is divided into two sections: Class 1 systems ("**must-have**") and Class 2 systems ("**important**") with timescales for these systems to support the business.

The following are critical **must-have** to enable the company to function.

a) Access to phones. This must be within 24 hours of disaster.
b) Must have access to client database, within 48 hours of the disaster.
c) Must have access to internet. This must be within 24 hours of disaster.
d) Access to accounts to maintain cash flow.

The following are the important to the business but not critical.

a) Access to staff working desktops. This can take up to 5 working days.
b) Access to working office environment. This can take up to 1 month from disaster.

10. Directories.

This section of the plan contains a series of directories.

These directories contain the type of information which is most likely to change such as names, addresses, telephone numbers etc.

It is important to keep these directories up to date.

10.1. Emergency Services

Service	Phone	Address
Police		
Fire		
Hospitals		
Gas		
Gas Escapes (24 hours)		
Electricity		
Electricity Supply Enquiries (24 hours)		
Water		
Burst Pipes/ Emergencies (24 hour)		

10.2. Recovery Team Members

The staff for the Recovery Team is listed in Disaster Management Team list section as in 10.2.1. The team leader is the first name in the list.

10.2.1. Disaster Management Team: Members and Contacts

Name	Work Phone	Home Phone	Pager/other contact info
Ian Foster			
Adele Fincham			
Adam Gibson			

10.3. First Aiders

For First Aid during office hours, contact <Name> at <Contact Number>.

If a first aider is not immediately available, contact the Emergency ambulance service by dialing 999.

10.4. Vendor and Supplier Contacts

This section lists all the key vendors and suppliers who need to be contacted following a disaster.

Requirement	Contact/ Company	Phone /Fax (working hours)	Phone outside working hours	Contract no. if any
Field Service				
Hardware				

Data communications				
Voice communications				
Wide Area Network Equipment				
Software				
Office Equipment				
Furniture				
Banking				
Air Conditioning				
Fire Protection/ Detection				
Salvage Contracting Services				

11. Inventories

This section contains inventories of all computer hardware, software and other equipment.

11.1. Computer Hardware

Manufacturer	Model, Description, Number	Qty
	Servers	

	PCs	
	Disk drives	
	Printers	
	Network equipment	

11.2. Software Inventory

Supplier	Description	Qty	License no.

11.3. Other Inventory

Item	Description	Quantity