Procedure for

Business Continuity & Disaster Recovery Plan

Version 3.3

Document version control page

Prepared By

Version	Date	Author	Update Description
1	28/7/2008	Jenish	Initial issue.
1.1	18/12/2018	Jenish	Included 120 KVA generator Included Reliance internet service provider
			Removed Net4India internet service provider
1.2	27/1/2009	Jayaseelanj	Jenish Name removed (**Committee Members and contact details)**
1.3	2/5/2009	J.Jayaseelan	Mohan Thas Name removed (**Committee Members and contact details)**
1.4	3/20/2009	J.Jayaseelan	Karthiban Gnanasekaran (Quality Manager) and Ramgopal K (Assistant Project Manager) Name Added in (Committee Members and contact details)
			VSNL & BSNL Name Removed in (ICE contact numbers)
			Tulip Name Added in (ICE contact numbers)
1.5	4/23/2009	J.Jayaseelan	Mr. Madhavaswamy name and Jayakumar name removed (Committee Members and contact details)
1.6	5/26/2009	J.Jayaseelan	Rajendara Name and P V Raju name removed (Committee Members and contact details)
			Mani Kumaran PA. Name added in (Committee Members and contact details)
1.7	10/13/2009	J.Jayaseelan	Karthiban Gnanasekaran (Quality Manager) Name is removed from (Committee Members and contact details)
1.8	5/21/2010	J.Jayaseelan	Annamalai (Business Development Manger), Mohammed Sadiq M.S (Business Head), Dr. M. Suriya Narayana Moorthy (e Learning Manager
1.9	11/25/2011	Jayaseelan J	Point : 1 Udhaya Kumar P., Mani Kumaran PA., Annamalai, Vasu, name removed and k.Sesha, Mythili, Aravand , Kalaiselvan A,. Premchandar name Added in committee members and contact details in **1.BCP committee members**
			Point:2 ISM name changed to ISH,
			AEL Data BCP Unit Address Changed in **BCP Unit**,

2	1/26/2012	Jayaseelan J.	Mr. Sesha giri Name removed and Mr. M. suresh name added in **(Committee Members and contact details)**
2.1	7/23/2012	Jayaseelan J	Document Reviewed
			BCP Key Persons Committee Members AEL Data @ Vals, Dlf & Kakinada. Mentioned as location wise.
			Mr. Satya Narayana name added in 3. BCP Committee Members.
			"Committee Members and contact details:"
2.2	6/28/2013	Jayaseelan J	
			Ramgopal name removed from the Committee Members and contact details:
			Valasaravakkam name changed to Porur
			Local contact details are updated
2.3	25/09/2013	Jayaseelan J	Document reviewed
2.4	21/06/2014	Jayaseelan J	Document reviewed
			Mr. Premchandar name is removed from BCP Key Persons & Committee Members
2.5	1/8/2014	Jayaseelan J	Document reviewed and updated as per 27K:2013 requirment
2.6	22/06/2015	Jayaseelan J	Document reviewed
2.7	14/06/2016	Jayaseelan J	DLF unit Name removed and Document reviewed
2.8	15/11/2017	Santhosh S	Document reviewed
2.9	12/6/2018	Santhosh S	Document reviewed
3.0	10/7/2019	Santhosh S	Document reviewed
3.1	09/11/2020	Santhosh S	Document reviewed
3.2	06/12/2021	Santhosh S	Mr.Aravind and Mythili name is removed from Committee Members
3.3	02/12/2022	Santhosh S	Document reviewed

Reviewed and Approved By

Version	Date	Approved By	Owner
1	6th August 2008	R. Kumar	MR/CISO
1.1	12/18/2008	R .Kumar	MR/CISO
1.2	1/27/2009	R.Kumar	MR/CISO
1.3	2/5/2009	R.Kumar	MR/CISO
1.4	3/21/2009	R.Kumar	MR/CISO
1.5	4/23/2009	R.Kumar	MR/CISO
1.6	5/26/2009	R.Kumar	MR/CISO
1.7	10/13/2009	R.Kumar	MR/CISO
1.8	5/21/2010	R.Kumar	MR/CISO
1.9	11/26/2011	R.Kumar	MR/CISO
2	1/27/2012	R.Kumar	MR/CISO
2.1	7/23/2012	R.Kumar	MR/CISO
2.2	6/28/2013	R.Kumar	MR/CISO
2.3	9/25/2013	R.Kumar	MR/CISO
2.4	6/21/2014	R.Kumar	MR/CISO
2.5	1/8/2014	R.Kumar	MR/CISO
2.6	22/06/2015	R.Kumar	MR/CISO
2.7	14/06/2016	R. Kumar	MR/CISO
2.8	15/11/2017	R. Kumar	MR/CISO
2.9	12/6/2018	R. Kumar	MR/CISO
3	10/7/2019	R. Kumar	MR/CISO
3.1	09/11/2020	R. Kumar	MR/CISO
3.2	06/12/2021	R. Kumar	MR/CISO
3.3	02/12/2022	R. Kumar	MR/CISO

• Purpose

This document established, describes the immediate action to be taken to continue the business if any disaster occurs to the assets of AEL data, A.17 Information Security Aspects of business continuity management (A.17.1 information security continuity) & (A.17.2 Redundancies) requirement.

• Scope

This procedure applies to all assets identified within AEL data, No: 100, Kundrathur Main Road, Porur, Chennai – 600 116.

• BCP committee members

A committee is formed with the key persons, who at the time of any issues, with continuing the business, will communicate to all the other persons of the committee members.

Committee Members and contact details:

Name	Designation	Address	Mobile number	Telephone Number	Official E-mail ID	Personal E-mail ID
Santhosh S	Information Security System Administrator	5/a,103 cheran st, vigneswara nagar , Porur,Chennai - 600116	99402 44818	04448517689	Santhosh@aeldata.in	santhoshvs123@gmail.com
R Kumar	Managing Director / Chief Information Security Officer	130(O) / 6 (N), Defense Officers Colony, Nandhambakkam, Chennai – 600 032	99400 57511	044 22330360	rkumar@aeldata.com	promeo@gmail.com
M.Suresh (BCP Unit)	Admin Manager BCP Unit	9-81/11 Sai Residency Sarpavaram Junction, Raminayapete market, Maruthi Nagar, Kakinada – 533 005	09247651232	08842347488	Suresh.m@aeldata.com	sureshsridurga@gmail.com
Vinay Kumar R	AVP	29/21, Vyasar Nagar, 1st Street, Vyasar Padi, Chennai – 600 039	99400 57506	044 25516472	vinay@aeldata.com	vinayrvk@gmail.com
Shankaran K.	Production Head /Vendor Manager	Old no. 73/2, New no. 20, CIT Nagar, 1st cross street, Nandanam, Chennai - 600035.	9940057504	044 24352423	shankarank@aeldata.com	sankaran_vara@yahoo.co.in

Mohammed Sadiq M.S	Sr VP	#139/2, 6th Street, Union Carbide Colony, Kodungaiyur, Chennai – 600118	9840721288		mdsadiq@aeldata.com	sadiq.ms@gmail.com
Dr. M. Suriya Narayana Moorthy	Delivery Head - Projects	4/6, vignesh flats, Muthumariyaman Kovil Street, Valasaravakkam, Chennai 600 087	9500063840	9962738458 044 - 24863679	suriya@aeldata.com	Drsuriya06@gmail.com
Mr. Kalaiselvan A.	Project Manager	2/249 Giri Gori Nagar Manappakkam Chennai 600125	9600100245	9841950665	kalaiselvan@aeldata.com	kalaikalai@yahoo.co.in
Mr. Satya Narayana	Accounts Manager	5-74/2 Anjani Street, ground Floor. Santosh Nagar, Kakinada 533 005, Andhra Pradesh,	09441463503		nvvsatya@andhraelec.com	

The committee will be headed by ISH.

BCP Key Persons Committee Members AEL Data @ Porur : Mr. Sadiq, Mr. Vinay, Mr. Aditya, Mr. Suriya, & Mr Subramanian Mr. Shankaran, , Mr. Kalaiselvan & Mr. Santhosh and Mr. Muthukrishnan

BCP Key Persons Committee Members AEL Data @ Kakinada: Mr. Suresh & Mr. satya Narayana.

The BCP procedure along with the Employee details & vendor details (hardware & software) will be sent to their personnel mail ID. So that, in case
of emergency, they can retrieve the data from their personnel mail for acting towards the disaster. Whenever, there is any update in any of the BCP / Employee list / Vendor list, ISH will ensure to send all the 3 documented information's to all the committee members' personnel mail ID mentioned in the subject block as "**BCP worksheet version x.y**". The latest version of these documented information as hardcopy will be maintained at ISH, & CISO residence.

It is advised to all the committee members to have a separate folder in their personnel mail id to have the latest BCP documented

information's. Also, all the committee members are advised to have the ICE contact numbers in their mobile.
This document and the associated documented information's will be reviewed once in a month and updated if necessary and communicated to all the members.

• Procedure – Business Continuity Plan (needs & expectations of interested party) (internal & External issues)

This is a disaster recovery plan for AEL Data. The information present in this plan guides AEL Data management and technical staff in the recovery of computing and network facilities and customer data in the event that a disaster destroys all or part of the facilities. The primary focus of this document is to provide a plan to respond to a disaster that destroys or severely cripples AEL Data's computer systems. The intent is to restore operations as quickly as possible with the latest and most up-to-date data available. Data recovery efforts in this plan are targeted at getting the systems up and running with the last available off-site backup from the Kakinada disaster recovery facility. Significant effort will be required after the system operation is restored to (1) restore data integrity to the point of the disaster and (2) to synchronize that data with any new data collected from the point of the disaster forward.

Personnel

Immediately following the disaster, a planned sequence of events begins. Key personnel are notified and recovery teams are grouped to implement the plan. Personnel currently employed are listed in the plan. However, the plan has been designed to be usable even if some or all of the personnel are unavailable.

Salvage Operations at Disaster Site

Early efforts are targeted at protecting and preserving the computer equipment. In particular, any storage media are identified and either protected from the elements or removed to a clean, dry environment away from the disaster site

Designate Recovery Site

At the same time, a survey of the disaster scene is done by appropriate personnel to estimate the amount of time required to put the facility (in this case, the building and utilities) back into working order. A decision is then made whether to use the Kakinada Site, a location some 500 Kilometers away from the scene of the disaster where computing and networking capabilities can be temporarily restored until the primary site is ready. Work begins almost immediately at repairing or rebuilding the primary site.

Purchase New Equipment

The recovery process relies heavily upon vendors to quickly provide replacements for the resources that cannot be salvaged. The AEL Data will rely upon emergency procurement procedures for equipment, supplies, software, and any other needs.

Begin Reassembly at Recovery Site

Salvaged and new components are reassembled at the recovery site. If vendors cannot provide a certain piece of equipment on a timely basis, it may be necessary for the recovery personnel to make last-minute substitutions. After the equipment reassembly phase is complete, the work turns to concentrate on the data recovery procedures.

Restore Data from Backups

Data recovery relies entirely upon the use of backups stored in Kakinada backup location. Early data recovery efforts will focus on restoring the operating system(s) for each computer system. Next, first line recovery of application and user data from the backup is done.

Restore Applications Data

Since some time may have elapsed between the time that the off-site backups were made and the time of the disaster, application owners must have means for restoring each running application database to the point of the disaster. They must also take all new data collected since that point and input it into the application databases. When this process is complete, the AEL Data computer systems can reopen for business. Some applications may be available only to a limited few key personnel, while others may be available to anyone who can access the computer systems.

Move Back to Restored Permanent Facility

If the recovery process has taken place at the Kakinada Site, physical restoration of the Porur building (or an alternate facility) will have begun. When that facility is ready for occupancy, the systems assembled at the Kakinada Site are to be moved back to their permanent home.

PREVENTION

As important as having a disaster recovery plan is, taking measures to prevent a disaster or to mitigate its effects beforehand is even more important. This portion of the plan reviews the various threats that can lead to a disaster, where our vulnerabilities are, and steps we should take to minimize our risk. The threats covered here are both natural and human-created:

- **Fire**
- **Flood**
- **Cyclones and High Winds**
- **Earthquake**
- **Computer Crime**
- **Terrorist Actions and Sabotage**

FIRE

The threat of fire in AEL Data Building is real and poses *a high risk*. The building is filled with electrical devices and connections that could overheat or short out and cause a fire. The computers within the facility also pose a target for arson from anyone wishing to disrupt AEL Data operations.

The Building is equipped with a fire alarm system, with ceiling-mounted smoke detectors scattered widely throughout the building. Smoke detectors are also placed beneath the raised floor of the machine room.

Hand-held fire extinguishers are placed in visible locations throughout the building. All Staff are trained in the use of fire extinguishers.

Staffs have undergone training and demonstrated proficiency in periodic, unscheduled fire drills. Regular reviews of the procedures are conducted to insure that they are up to date. Unannounced drills are conducted by Security Management Team.

FLOOD

The Building is located in an area surrounded by low ground. With the chance of large amounts of rain in the Chennai area especially during the monsoon months *would* create the threat of flooding.

CYCLONES AND HIGH WINDS

As AEL Data is situated along the cyclone prone region of the south east coast of India, damage due to high winds or an actual cyclone is a real possibility. A cyclone has the potential for causing the most destructive disaster we face.

While a fire can be as destructive as a Cyclone, there are very few preventative measures that we can take for Cyclones. Strong winds are often accompanied by heavy rain, so a double threat of wind and water damage exists if the integrity of the roof is lost.

Maintenance Services has large tarpaulins available in the area ready to cover sensitive equipment in case the building is damaged. Protective plastic covering should also *be* available *and* deployed over media racks to prevent water and wind damage. Operators are trained how to properly cover the equipment.

EARTHQUAKE

The threat of an earthquake in the Chennai area is medium and should not be ignored. Buildings in our area are not built to earthquake resistant standards so we could expect light to moderate damage from the predicted quake. An earthquake has the potential for being the most disruptive for this disaster recovery plan. If the Building is damaged, it is highly unlikely that the Kakinada Site may also be similarly affected. Restoration of computing and networking facilities following a bad earthquake could be very difficult and require an extended period of time due to the need to do large scale building repairs.

The preventative measures for an earthquake can be similar to those of a Cyclone. Even if the building survives, earthquakes can interrupt power and other utilities for an extended period of time. Standby power generators ha*ve* been leased to provide power while commercial utilities are restored.

Maintenance Department has plastic sheeting available in the machine room area ready to cover sensitive electronic equipment in case the building is damaged. Protective covering will be deployed over media racks to prevent water and wind damage. Operators have been trained how to proper*ly* cover the equipment.

COMPUTER CRIME

Computer crime is becoming more of a threat as systems become more complex and access is more highly distributed. With the new networking technologies, more potential for improper access is present than ever before. Computer crime usually does not affect hardware in a destructive manner. It may be more insidious, and may often come from within. A disgruntled employee can build viruses or time bombs into applications and systems code. All systems have security products installed to protect against unauthorized entry. All systems are protected by passwords. All users are required to change their passwords on a regular basis. All systems *should* log invalid attempts to access data, and *the* system administrator reviews these logs on a daily basis.

All systems are backed up on a periodic basis. Physical security of the data storage area for backups is implemented. Standards have been established on the number of backup cycles to retain and the length of their retention.

Policies and procedures are strictly enforced when violations are detected *(?)*. Operators are regularly told the importance of keeping their passwords secret.

TERRORISTIC ACTION AND SABOTAGE

The AEL Data's computer systems are potential targets for terrorist actions, such as a bomb. The threat of kidnapping of key personnel also exists. Good physical security is extremely important. However, terrorist actions can often occur regardless of in-building security, and they can be very destructive. A bomb placed next to an exterior wall of the machine room will likely breach the wall and cause damage within the room.

The building is adequately lit at night on all sides. All doors into the area are strong and have good locks. Only those people with proper security clearances are permitted into the building. Suspicious parties should be reported to the police (they may not be terrorists, but they may have theft of expensive computer equipment in mind).

Sl. no	risks and opportunities	Effect on Business (needs & expectations)	Impact	Preventive controls	Controls Identified if preventive Controls fails & Information Security and the Business Continuity Plan	Recovery time
1.	Servers destroyed by fire – Data will be lost	Business will be affected moderately – production will be stopped as data are lost	Major	The servers are placed in a closed environment where room temperature is maintained between 16-24°C.	2x2kg Auto fire sensing sprinklers are installed which will control fire to the entire server room if the smoke / flame / fire are at 60°C. A replacement server will be bought for production continuation	12 hours
				Access to server room is limited so that there will not be a chance of physical movement of servers, by unauthorized persons, which may lead to internal short-circuit	Everyday back-up is taken in the tape & sent to registered office. New server will be installed and data will be transferred for production	48 hours
					For online projects, BCP unit people were trained and production will be continued until recovery	1 hour
2.	Server room fire – electrical equipments including network connections will be fired	Business may be affected severely – chance of fire extending to other areas and damage the entire assets. Also production will be affected	Major	2x2kg Auto fire sensing Extinguisher's are installed which will control the fire to the entire server room if the smoke / flame / fire are at 60° so that, the fire will not be extended to other rooms / areas	For online projects, people at BCP unit were trained and production will be continued until recovery	1 hour
					Prioritize other projects based on customer delivery requirement and transfer the data from back-up media to local hard disk of the work station	24 hours
				The patricians are made up of non-explode able MDF wood which has the fire resistivity up to 425°C. The frames are made up of aluminium which is a highly fire resistivity alloy	A new server and all other equipments will be procured and the original setup will be retained	72 hours
3.	Entire facility fire – all the assets will not be able to use. People will not be able to access the facility at least for 5 days	Business will be affected severely – huge data, assets and production will be lost	Major	Air-conditioned environment is maintained ensuring that the temperature is maintained between 24-28°C.	For online projects, people at BCP unit were trained and production will be continued until recovery	1 hour
				The patricians are made up of non-explode able MDF wood & gypsom boards with glass wool which has the fire resistivity up to 425°C. The frames are made up of aluminium which is a highly fire resistivity alloy	A team of the Chennai employees will be moved to BCP location for production continuation.	48 hours
					The Chennai facility will be renovated for the original setup	14-20 days

				Fire extinguishers are identified, located and personals are trained to use		

Sl. no	risks and opportunities	Effect on Business (needs & expectations)	Impact	Preventive controls	Controls Identified if preventive Controls fails & Information Security and the Business Continuity Plan	Recovery time
4.	Virus/ Malicious attack on our network – data will be corrupted	Business will be affected moderately – production will be stopped as data are lost	Medium	Anti-virus software is being installed and updated once in 15 days in all the systems	Back-up is taken and up gradation will be done in the server and data will be transferred	24 hours
5.	Natural calamities – Flood / Cyclone – people will not be able to access the facility at least for 3 days	Business will be affected moderately – production will be affected	Medium	-NIL- as incidents are "UNPREDICTABLE"	For online projects, people at BCP unit were trained and production will be continued until recovery	1 hour
					Production will be started at BCP unit if the situation is suspected to continue for more than 4 days	24 hours
	Tsunami	Nil	Low	Porur is located at an altitude of 52 feet from MSL and 15.7 km from sea	-	-
	Earthquake – people will not be able to access the facility for at least 3 days	Business will be affected moderately – data, all assets and people are safe	Medium	-NIL- as incidents are "UNPREDICTABLE"	For online projects, people at BCP unit were trained and production will be continued until recovery	3 hours
		Business will be affected severely – data, all assets and people are not safe / all assets and data are damaged	Major		For online projects, people at BCP unit were trained and production will be continued until recovery	3 hours
					Entire production will be started at BCP facility by hiring people (if required) until everything at Chennai facility is normal	120 hours
6.	Political unrest/ issues (bandh / strike / local holiday etc) – people will not be able to access the facility	Business will be affected moderately – not more than 2 days	Medium	-NIL- as incidents are "UNPREDICTABLE"	For online projects, people at BCP unit were trained and production will be continued until recovery	1 hour
		Business will be affected severely – more than 2 days	Major		Entire production will be started at BCP facility by hiring people (if required) until everything at Chennai facility is normal	120 hours

Sl. no	risks and opportunities	Effect on Business (needs & expectations)	Impact	Preventive controls	Controls Identified if preventive Controls fails & Information Security and the Business Continuity Plan	Recovery time
7.	Terrorist attack – people will not come and access the facility	Business will be affected moderately – not more than 2 days	Medium	-NIL- as incidents are "UNPREDICTABLE"	For online projects, people at BCP unit were trained and production will be continued until recovery	1 hour
		Business will be affected severely – more than 2 days	Major (more than 2 days)		Entire production will be started at BCP facility by hiring people (if required) until everything at Chennai facility is normal	120 hours
		Business will be affected severely – attacked at the facility	Major		Entire production will be started at BCP facility by hiring people (if required) until everything at Chennai facility is normal	120 hours
8.	Electrical problem	Business will be affected moderately – internal	Moderate	-NIL- as incidents are "UNPREDICTABLE"	Electricians are employed and also contracted.	2 hours
		No impact over the business – external	Minor		UPS with 1 hour capacity is at place and generator of 125 KVA is at place electrical team is in place for maintenance	Immediate
9.	Industrial unrest/ strike	Business will be affected severely – production will be affected	Major	Salaries are provided based on industry standards	For online projects, people at BCP unit were trained and production will be continued until recovery	1 hour
				Promotional activities are provided	BCP unit people was trained for all the major projects and a low volume will be produced everyday by 10 people on a rotation of 5 people everyday. On requirement, the production will be ramped up by providing necessary training.	24 hours
				No labour union	Existing people will be counselled for rejoining	48 hours
					Entire production will be started at BCP facility by hiring people (if required) until everything at Chennai facility is normal	120 hours
					If counselling failed, fresh recruitments will be made and the production will be ramped up	504 hours (21 days)

Sl. no	Test	Effect on Business (needs & expectations)	Impact	Preventive controls	Controls Identified if preventive Controls fails & Information Security and the Business Continuity Plan	Recovery time
1.	Redundancy Test for DR Site & Primary Site	Business will be affected moderately – production will be stopped as data are lost	Minor	DR Site Backup Restoration Test done for the infrastructure requirement in AEL Data (A.17 Information Security Aspects of business continuity management (A.17.1 information security continuity) & (A.17.2 Redundancies)	Every 6 months ones Redundancy Backup Test at DR Site and Primary Site conducting for Internet and VPN connectivity	10 mins
				DR Site Backup Restoration Test done for the Employee requirement in AEL Data (A.17 Information Security Aspects of business continuity management (A.17.1 information security continuity) & (A.17.2 Redundancies)	Every 6 months ones Redundancy Backup Test at DR Site and Primary Site conducting for Employee requirement	1 hour
					Every 6 months ones Redundancy Backup Test at DR Site and Primary Site conducting for Power Backup requirement	1 hour
					Every activity of Burning the Taps and DVD's Restoration Test can be done. To check the Redundancy Backup Primary Site to ensure the processed Data is well preserved	Every Burning Activity and Based on the size of Volume of Data

BCP unit:

AEL Data
5-74/2 Anjani Street, 2nd Floor.
Santosh Nagar,
Kakinada 533 005,
Andhra Pradesh, India.
Tel : +91 884 235 3248

Registered Office:

AEL Data
130, Defence Officers colony,
Guindy
Chennai
Ph: 044- 22330360

ICE contact numbers:

Police station: Porur (044) 23452767

Nearest hospital: Sri Ramachandra Medical Centre , No 1, Ramachandra Nagar, Porur, Chennai - 600116Call: (044) 24765512

Nearest Fire service station:

Address 1: No 167, Kumananchavadi, Poonamallee High Road, Poonamallee, Chennai – 600056 call: 26274700

Address 2: Koyambedu Market, Koyambedu, Chennai - 600107 Call: 24792610

EB office: Phone: 044 – 24826554 ,Address: #110/33/11, Kundrathur Rd, Porur, Chennai -600116 call: – 24860694
Internet: Airtel: 1800-103-0121 / Aircel: 18001033003 / Reliance (Kakinada): 180030008383