1.0   Objective

1.1   To formalize Infinit-O's Business Continuity Management Program and to provide guidelines for developing, maintaining and exercising its Business Continuity Plan (BCP).

1.2   This policy establishes the basic principles and framework necessary to ensure emergency response, resumption and recovery, restoration and permanent recovery of the organization's operations and business activities during a business interruption event.

2.0   Scope

2.1   This applies to all team members, information-processing facilities and corresponding IT systems when any of the following scenarios, including, but not limited to, natural disaster, power outage, hardware/telecommunications failures, data corruption, force majeure situations, occur.

2.2   This policy provides guidance for the Resumption and Recovery of time sensitive business operations in accordance with pre-established timeframes as well as ensuring that adequate plans are in place for the less time sensitive business operations.

3.0   Provisions

3.1   Business Impact Analysis and Risk Assessment

    3.1.1   BCT shall conduct a bi-annual asset risk assessment, analysis and treatment.
        3.1.1.1 The criticality of each identified scenarios is determined using Probability and Impact ratings stated under 4.3.4 and 4.3.5 of our CPP-IOI-0013. Please see APPENDIX A Disaster Recovery and Business Continuity Plan Matrix.

    3.1.2   BCT finalizes and presents the recommended action items to EXECOM for approval.

3.2   Business Continuity Plan (BCP)

    3.2.1   Infinit-O develops and maintains its BCP to ensure its recovery from any disruptions to its business operations and to provide the ability to recover its critical processes within the agreed timelines.

    3.2.2   BCP should address any organizational vulnerability that may compromise the confidentiality, integrity and availability of the company and/or client-supplied data and information.

    3.2.3   The recovery plans include appropriate action items for different scenarios. These action items are identified, activated and implemented according to specified conditions and timelines.

    3.2.4   Alternate approaches for resumption of work including remote work, working from other office buildings, etc., shall be identified for the affected teams.

    3.2.5   BCP includes emergency, fallback, temporary operational and resumption procedures.

    3.2.6   BCP should indicate how service restoration is prioritized.

3.3   Resumption and Recovery Plans for People Assets

3.3.1   HR is responsible for establishing a clear chain of command starting with the EXECOM for business continuity.

3.3.2   Each VP is responsible for their group's chain-of-command planning. The plan must be communicated to HR and BCT.

3.3.3   BCT must ensure the fulfillment of chain of command planning by the VPs.

3.3.4   Each project team shall implement and maintain a basic communication plan for all their team members for emergency response and business continuity. Guidance on what constitutes a basic communication plan shall follow a standard to be developed and issued jointly by Execom and BCT. Confidentiality of team members' personal contact information for this purpose shall be managed in compliance with the Infinit-O's Security and HR policies and practices.

3.3.5   BCT shall identify the designated front-runners for each project teams and the alternate team members who perform functional responsibilities in the absence of the front-runners. Some team members may be required to work from remote offices or from home.

3.3.6   BCT shall work with HR to develop clear guidance on how the Shared Services Teams members shall work their time during a crisis. These team members may be directed to suspend their regular duties until the operations are restored at a permanent site or Execom provides some alternate direction.

3.4   Resumption and Recovery Plans for Facilities and Office Space

3.4.1   BCP Procedures contain the coordinated strategy involving plans, policies, procedures, and technical measures that enable the recovery of IT systems, operations, and data that is identified as critical. EXECOM shall also work with other teams that are responsible for development and maintenance of the technology and information that support critical business processes of Infinit-O.

3.4.2   EXECOM must provide a safe, easily accessible and operational location with adequate resources for the team members to report to and initiate operations during a disruption.

3.4.3   The alternate facility must have a power supply, Internet connection and phone lines to support efficient response during a crisis. The alternate facility must prove adequate office space and alternate communication links with the clients.

3.4.4   BCT shall ensure that the level of security controls at the main site is replicated in the alternate site.

3.4.5   For business restoration and permanent recovery, EXECOM shall work closely with BCT, IT and Shared Services Teams to coordinate the activities in restoring Infinit-O's operations and ultimately returning to an original or transferring to a new permanent operating site.

3.5   Resumption and Recovery Plans for IT Systems

   3.5.1   Infinit-O's network architecture and telecommunications shall ensure redundancy and ability to cope with a disruption.

   3.5.2   The company policy on Business Continuity Management Program is integrated in IT policies, budget and implementation decisions. IT budget guidelines shall take into account good practices concerning continuity planning and readiness.

   3.5.3   For any new application development, BCP should be integrated in all phases of the IT project life cycle that includes Business Requirements, System Architecture, Design, Construction, Testing, Implementation, Maintenance and Retirement.

3.6   Testing

   3.6.1   BCP should be tested at least annually to ensure credible recovery preparedness. Execom shall determine the scope, objectives, and measurement criteria of each test on a *per event* basis. Test results shall be shared with BCT.

   3.6.2   The testing schedule and results are found in APPENDIX B of this document.

3.7   Corporate Communication

   3.7.1   External communication during a time of crisis is very critical. SVP-Client Solutions Group and Client Solutions VPs are responsible for communicating with their respective clients.

   3.7.2   HR shall be responsible for communicating with the Managers and Team Leaders who, in turn, will notify their respective team members.

   3.7.3   HR must update the Team member directory quarterly.

3.8   Training

   3.8.1   Business Continuity training for BCT, IT and Shared Services Teams is essential for effective resumption and recovery of operations.

   3.8.2   BCT shall ensure training to keep current in business continuity and Infinit-O processes, latest technologies, international standards and regulations that guide the development and enhancements of the BCP.

3.9   BCP Maintenance and Management Reporting

   3.9.1   BCP shall be updated bi-annually or as often as changes require. These changes may include acquisition of new equipment, key processes and systems, key team members and their contact numbers, business strategy, resources, suppliers and top clients.

   3.9.2   All major updates should be incorporated as soon as possible and is not held to satisfy a pre-arranged schedule.

3.9.3   BCT shall report the status and progress of BCP during the Quality & Information Security Review Meetings with Execom every six (6) months or after every test.

3.10   Policy Compliance

3.10.1   Consistent compliance with this policy is essential to its effectiveness. Infinit-O management and team members are expected to adhere to this policy and to follow it consistently.

3.10.2   BCT shall assess the preparedness of the organization and report to Execom during the Quality & Information Security Review Meetings with Execom every six (6) months or after every test. The assessment includes the qualifications of Infinit-O's exposure, including but not limited to, the resumption of time-sensitive operations and recovery of project teams.

3.10.3   Periodic internal audit is conducted.

4.0   Responsibility

4.1.1   EXECOM is responsible for the approval of the BCP policy, planning and governance. They are also responsible for provision of sufficient financial resources to address the identified requirements during a crisis.

4.1.2   MANCOM is responsible for disseminating the appropriate announcements to their subordinates and assist EXECOM and other admin teams in movement of action plans.

4.1.3   Business Continuity Team (BCT), who is composed of the Client Solutions VPs, IT and Shared Services Teams have the overall responsibility to create the specific plans to provide leadership and guidance that ensures the appropriate consistency, coordination and compliance among the team heads and team members.

4.1.4   IT Team (IT) is responsible for the final selection of the alternate site and provision of IT resources during a disruption type that needs relocation. IT Team should ensure that any information unavailability/loss is at an acceptable level.

4.1.5   Shared Services Team (SST), who is composed of HR, F&A and SSP Teams, is responsible for the activation of the BCP upon receipt of notice and approval from Execom. This team provides overall support to affected teams to ensure personnel safety and smooth execution of the BCP.

4.1.6   Human Resources (HR):
4.1.6.1   Monitor the calamities.
4.1.6.2   Notify Execom on the status of calamities, events and/or disruptions.
4.1.6.3   Release pertinent advisory to all VPs, Team Leaders, upon receipt of instructions from Execom.

4.1.7   EXECOM is responsible for decision-making.

4.1.8   SVP-Client Solutions Group
4.1.8.1   Is responsible for composing the email advisory as well as its release to all clients.
4.1.8.2   If email is unavailable, call all affected clients.
4.1.8.3   Client Solutions Heads may assist if there's time constraint.

4.1.9 VPs, in coordination with their respective Managers and/or Team Leaders are responsible for disseminating the appropriate announcement to their subordinates.

4.1.10 F&A Team is responsible for the release of any required funds, when necessary.

4.1.11 SSP Team is in charge of provision of any required resources including the relocation area/s.

4.1.12 The IT Team is responsible for setting up offsite offices and restoration of services in the facilities.

5.0 Frequency

5.1 Testing – annually
5.2 Review – every 6 months
5.3 BCP Activation – when needed

6.0 Distribution

Execom
Business Continuity Team

7.0 Usage

7.1 Standard Service Level Agreement with Client on:
7.1.1 Key Result Areas
Refer to each Team's Deliverables.

7.2 Force Majeure
The obligations of the parties shall be suspended to an extent and for the period that performance is prevented by force majeure. "Force Majeure" means acts of God, laws, regulations or orders of any government or governmental entities, judgments or orders of any court of competent jurisdiction, acts of war or conditions arising out of or attributable to war, whether declared or undeclared, riots, terrorism or other criminal activity, insurrections or rebellions, fire, explosions, earthquake, storm, flood, volcanic eruption, drought or other severe and unusual adverse weather conditions; accidents; or any other cause similar to the foregoing.

7.3 Call Tree
7.3.1 SVP-Shared Services will initiate the call tree by notifying all VPs, and IT Manager through SMS or Call
7.3.2 VP's will then notify their respective Managers and Team Leaders (when applicable).
7.3.3 Team members must respond via SMS or Call within 20 minutes upon receipt of the notification.
7.3.4 Managers and/or Team leaders must continue to reach team members if no response is received within 20 minutes.
7.3.5 Managers and/or team leaders will submit status report to HR-ER copy VP's and SVP-Shared Services within one hour after they receive the notification. New updates must be provided as they come.

7.4 Events

7.4.1 Event: No Internet Connection on any ISP

7.4.1.1 Team Member or Team Leader/Account Handler: Report the problem to IT through the Ticketing System. Send an email to otrs@infinit-o.com.

7.4.1.2 IT Team: Route the network to backup DSL line 1.

7.4.1.3 IT Team: Identify potential cause(s) of failure.

7.4.1.4 IT Team: If the cause is external, coordinate with carrier to seek update on the nature of the failure and the expected time of restoration of service.

7.4.1.5 IT Team: If the cause is internal, troubleshoot.

7.4.1.6 IT Team: If all available internet connections failed and the event cannot be resolved within thirty (30) minutes, inform Team Leader/Account Handler.

7.4.1.7 Team Leader/Account Handler: If disruption will affect Client Deliverables, inform the Management Team regarding the event, the impact and the expected time of restoration.

7.4.1.8 Management Team: Assess if the affected Team(s) should be relocated. If relocation is required, inform Team Leader/Account Handler and refer to 8.0 Relocation.

7.4.1.9 Team Leader/Account Handler: Inform the Client regarding the event, the expected time of restoration and relocation when applicable.

7.4.2 Event: Workstation and Server Problems

7.4.2.1 Due to Viruses, Malwares and Spywares

7.4.2.1.1 Team Member or Team Leader/Account Handler: Immediately shutdown the computer and notify the IT team though the ticketing system via another terminal or via phone.

7.4.2.1.2 IT Team: Disconnect the (suspected) virus infected computer from the network.

7.4.2.1.3 IT Team: Commence virus clean-up.

7.4.2.1.4 IT Team: Disseminate information about new computer viruses to team members to increase awareness and reduce potential risk of infection.

7.4.2.1.5 IT Team: If the event or virus cannot be cleaned within thirty (30) minutes, deploy spare computer.

7.4.2.2 Not Virus, Malware or Spyware Related Problems

7.4.2.2.1 Team Member or Team Leader/Account Handler: Report the problem to IT through the Ticketing System. Send an email to otrs@infinit-o.com.

7.4.2.2.2 IT Team: Troubleshoot.

7.4.2.2.3 IT Team: If the problem cannot be resolved within thirty (30) minutes, deploy spare workstation.

7.4.2.2.4 IT Team: Upon resolution, member's workstation is restored and the deployed spare unit is pulled out.

7.4.3 Loss of Data in File Servers

7.4.3.1 Team Member or Team Leader/Account Handler: Report the problem to IT through the Ticketing System. Send an email to otrs@infinit-o.com.

7.4.3.2 IT Team: Assess and identify specific lost data.

7.4.3.3 IT Team: Retrieve back-up copy of lost data and start the restoration process.

7.4.3.4 IT Team: If the file cannot be restored within sixty (60) minutes, Inform the team member of estimated time of restoration.

7.4.3.5 Team Leader/Account Handler: If disruption will affect Client Deliverables, inform the Management Team and Client regarding the event, the impact and the expected time of restoration.

7.5 Event: Phone Problems

7.5.1 Team Member: Use the secondary dialing procedure.

7.5.2 Team Member or Team Leader/Account Handler: Report the problem to IT through the Ticketing System if problem persist with the secondary route/dialing procedure . Send an email to otrs@infinit-o.com.

7.5.3 IT Team: Troubleshoot.

7.5.4 IT Team: If the event cannot be resolved within thirty (30) minutes, inform Team Leader/Account Handler.

7.5.5 Team Leader/Account Handler: If disruption will affect Client Deliverables, inform the Management Team regarding the event, the impact and the expected time of restoration.

7.5.6 Management Team: Assess if the affected Team(s) should be relocated. If relocation is required, inform Team Leader/Account Handler and refer to 8.0 Relocation.

7.5.7 Team Leader/Account Handler: Inform the Client regarding the event, the expected time of restoration and relocation when applicable.

7.6 Event: Power Failure at Facility:

In the event of a power failure, Pacific Star Building is equipped with two groups of generators that provide 100 percent back-up power for the building. The generators are controlled by an Automatic Transfer Switch (ATS) and an 8-second interval delay is experienced when transferring from one source of power to another. (Ref. Pacific Star Building House Rules)

7.6.1 IT Team:

7.6.1.1 Ensure that all resources for possible relocation must be ready for transport.

7.6.2 SSP:

7.6.2.1 Emergency lights' life when on is __ hours. Ensure that these are always in working condition.

7.6.2.2 Coordination with Pacific Star building administration teams on estimated time of return of power and other back-up systems.

7.4.2.4 If the event cannot be resolved within thirty (30) minutes, inform the Management Team, Team Leader/Account Handler.

7.6.3 Team Leader/Account Handler and/or Client Solutions Head:

7.6.3.1 If the disruption will affect Client Deliverables, inform the Management Team regarding the event, the impact and the expected time of restoration.

7.6.3.2 Inform the Client regarding the event, the expected time of restoration and relocation when applicable.

7.6.4　Management Team:

　　　　7.6.4.1　If the power outage lasts more than 12 hours, assess if the affected Team(s) should be relocated.

　　　　7.6.4.2　If relocation is required, inform Team Leader/Account Handler and/or Client Solutions Heads and refer to 7.17 Relocation Procedure.

7.6.5　Client Solutions Group Director:

　　　　7.4.5.1　Identify priority projects which are time sensitive, dealing with live data and/or with contractual obligations.

　　　　7.4.5.2　These priority projects must be relocated asap when the event threatens the deliverables of the account/s.

7.7　Event: Unauthorized Personnel at Facility Premises

　　　　Client Solutions Head/Team Leader/Account Handler:

7.7.1　Once unauthorized entry has been discovered, contact the Building Security Guard as soon as possible.

7.7.2　If the Building Security Guard cannot be reached, contact the local police station.

7.6.3　In the event that none of the Management Team is available, assume ownership of the event.

7.8　Event: Accessible Facility but Inaccessible Production Area

7.8.1　Support Groups, Affected Team Leader, and Team Leader/Account Handler:

　　　　7.8.1.1　Assess the extent of the event.

　　　　7.6.2.2　Create a plan if affected Team(s) can be moved to another production area or another area in the Facility.

7.8.2　Team Leader:　Inform Team Members of the Plan.

7.8.3　All:　　　　Execute plan.

7.8.4　IT Team: If the event cannot be resolved within thirty (30) minutes, inform Team Leader/Account Handler.

7.8.5　Team Leader/Account Handler: If disruption will affect Client Deliverables, inform the Management Team regarding the event and the impact.

7.8.6　Management Team:

　　　　7.8.6.1　Assess if the affected Team(s) should be relocated.

　　　　7.8.6.2　If relocation is required, inform Team Leader/Account Handler and refer to 8.0 Relocation.

7.8.7　Team Leader/Account Handler: Inform the Client regarding the event, the expected time of restoration and relocation when applicable.

7.9　Event: Fire in office premises

7.9.1　Team member that notices the fire should attempt to contain the fire using the fire extinguishers situated around the office.

7.9.2　If the fire uncontainable, sound the fire alarm and alert the proper authorities.

7.9.3　If fire is outside of office premises, assess the situation and determine if evacuation is needed.

7.9.4　If evacuation is needed, coordinate with Pacific Star Building admin personnel on proper procedure.

7.9.5　Emergency evacuation plan and locators are situated in the hallways outside the hallways.

7.9.6　HR:

　　　　7.9.6.1　Must ensure safety of all team members

　　　　7.9.6.2　Must coordinate with other admin teams on emergency next steps and procedures.

　　　　7.9.6.3　Assist any team member in need of medical assistance.

7.9.7　SSP

7.9.7.1 Directly coordinate with Pacific Star building admin and local authorities on status and size of the fire.

7.9.7.2 In the event of an evacuation, the facilitation of SSP team members will be needed.

7.9.8 IT

7.9.8.1 Must secure the company equipment and ensure minimal damage and containment.

7.9.8.2 Team must also directly coordinate with other admin teams on emergency next steps and procedures.

7.9.9 MANCOM

7.9.9.1 Committee must assist team members and other admin teams in need.

7.9.9.2 If the emergency will affect client deliverables, MANCOM must inform the clients of the situation.

7.9.10 EXECOM

7.9.10.1 Committee must take charge of executive decision making and provide assistance to team members and other admin teams in need of assistance.

7.10 Event: Earthquake

7.10.1 Sound the alarm (fire alarm) or emergency whistle located in the first aid stations around the office.

7.10.2 Duck, cover and hold position until earthquake subsides.

7.11 HR

7.11.1 HR team must ensure safety of all team members.

7.11.2 Must coordinate with other admin teams on emergency next steps and procedures.

7.11.3 Assist any team member in need of medical assistance.

7.12 SSP

7.12.1 Directly coordinate with Pacific Star building admin and local authorities on damage assessment, medical situation and evacuation plan.

7.12.2 In the event of an evacuation, the facilitation of SSP team members will be needed.

7.13 MANCOM

7.13.1 Committee must assist team members and other admin teams in need.

7.13.2 IF the emergency will affect client deliverables, MANCOM must inform the clients of the situation.

7.14 EXECOM

7.14.1 Committee must take charge of executive decision making and provide assistance to team members and other admin teams in need of assistance.

7.15 Event: Inaccessible office premises due to severe typhoon or flood

7.15.1 All teams: Monitor the weather advisory from local weather agency and news bureau.

7.15.2 SSP, EXECOM and MANCOM: Assess if there are other threats to the office location.

7.15.3 MANCOM and EXECOM: Determine if team members can report to office location or if work from home will be allowed.

7.15.4 HR: must ensure that all team members stranded in office premises are provided with ample food and shelter.

7.15.5 MANCOM and EXECOM: Contact client point person via mobile phone or other channels and advise of situation including estimated time to restore normal operations.

7.16 Phone Problems

7.16.1   Team member: Use the secondary dialing procedure
7.16.2   Team members or TL/account handle: Report problem to IT through the ticketing system (otrs@infinit-o.com) if problem persists.
7.16.3   IT team: troubleshoot the situation. If problem cannot be addressed, inform MANCOM.
7.16.4   MANCOM: If disruption will affect client deliverables, inform clients through alternative sources including estimated time of restoration.

7.17   Relocation to Another Facility

In the event that the Management Team has decided to relocate the affected Teams to another location outside Infinit-O facility:

7.17.1   Support Groups and Client Solutions Group Director: Create a Relocation Plan which includes:
7.17.1.1   Location – nearby hotels and serviced residences with generator and WiFi that can accommodate at least 10 people in a room or area.
7.17.1.2   Team Affected – priority projects are those which tasks and deliverables are time sensitive, dealing with live data and/or with contractual obligations
7.17.1.3   Time frame for Relocation – must be done within _____ minutes
7.17.1.4   Required Equipment – PCs and headsets
7.17.1.5   Required Supplies including food for staff
7.17.1.6   Budget
7.17.2   HR/Client Solutions Group Director: Inform affected Client Solutions Head, Team Leaders/Account Handlers of the agreed plan.
7.17.3   Client Solutions Head, Team Leader/Account Handler: Inform members of the agreed plan.
7.17.4   IT Team:
7.17.4.1   Prepare the resources for transport to the relocation area.
7.17.5   All: Implement agreed plan.

8.0   Evacuation for Legazpi City Team Members:

8.1   Site director must have direct communication with local government
8.2   All team members are encouraged to monitor local news and regional developments.
8.3   Designated relocation sites will be identified by the local government.
8.4   All team members must evacuate office premises upon order of local government.
8.5   All equipment inside office premises must be secured. The site director with the assistance of IT team members on duty will securely lock all exit and entry points into office premises. The site director will be in charge of safekeeping the key.
8.6   HR team member will maintain communications with ManCom and ExeCom team members in Manila.
8.7   Team members will proceed to the nearest designated evacuation area.

9.0   General Evacuation Procedures
9.1   Become familiar with your building and know the location of emergency exits and one nearest to you.
9.2   Notify appropriate authorities in any emergency situation.
9.3   If evacuation is necessary, authorities may direct you to the identified evacuation site.
9.4   Remain calm and try to keep others calm.
9.5   Exit the building use stairwells. Close and secure all doors behind you.
9.6   Proceed to the designated meeting area. Await further directions and instructions from authorities.

9.7 Be of assistance to others if needed.

9.8 Notify the first responding agency of any disabled, trapped or injured person.

10.0 Emergency Contact Details for Legazpi team members

PNP – Legazpi Police Station	Tahao Road, Legazpi City	+63 (52) 480 0168
Legazpi City Fire Station	Albay District, Legazpi City	+63 (52) 821 7941
Public Safety Office/Civil Security Unit	Motorpool, Airport Site, Legazpi City	+63 (52) 480 0162
Embarcadero Mall Admin		052 481 1000

11.0 Restoration of Services

In the event that Infinit-O's facilities are inoperable for longer than a day due to force majeure or manmade disruptions:

8.1 Management Team/BC Team: Create a Restoration Plan which includes:
- 8.1.1 Assessment of the Extent of Damage
- 8.1.2 Priority of Restoration -
- 8.1.3 Time frame of Restoration
- 8.1.4 Budget.

8.2 Finance Team: Coordinate the needed budget for the BCP with the Board of Directors .

8.3 President: Release Funds to either Finance and/or Procurement.

8.4 Finance Team: Contact BCP Insurance for possible coverage of loss when applicable.

8.5 All: Implement agreed plan.

8.6 Operations Head: Once restoration is complete, inform affected Team Leaders.

8.7 Team Leader: Inform team members.

12.0 References

Infinit-O ISO Documents

13.0 Records

Management Review Records

APPENDIX A

	Company Policy & Procedure Manual **Business Continuity Plan (BCP)** Ref. No.: CPP-Infinit-O_0010	Version	1.0	Page	12	Of	25
		Prepared	C. Malay		27-Jun-2104		
		Approved	Execom		30-Jun-2014		
		Filename	CPP-Infinit-O_0010_V1_Business Continuity Plan (BCP)				

Disaster Recovery and Business Continuity Plan Matrix

PROBLEM SCENARIO	CRITI-CALITY	CONTROL CONCERN	PROBA-BILITY	CONTROL MEASURE/CONTINUITY PROCEDURE	RESPONSIBILITY	TESTING FREQUENCY
Power Failure at Facility (May be a result of the following: Fire, Typhoon, Flooding, Earthquake	2 2	Disruption of normal operations Proximity Door systems unavailable during power outage (potential theft of company assets)	2	1. Building auto failover power source to Generator set 2. Secure periodic preventive Maintenance report from Building 3. Conduct periodic test of Proximity Door system's backup power/battery	1. Building Administrator 2. SSP 3. IT	Annual
Fire at Facility	2 2 2	Injury to/Loss of Life of facility occupants Disruption of normal operations Damage to Equipment	1 1 1	1. Assess extent of fire threat 2. Notify PACSTAR building admin 3. Utilize fire suppression equipment to contain fire threat 4. Depending on fire threat, initiate facility evacuation procedures 5. Where individuals have sustained injuries, administer first aid and coordinate with local emergency agencies once outside the facility 6. Conduct periodic fire drills 7. Implement CPP-HR-0404 1. Minimize damage thru power disconnection and system shutdown as deemed necessary	1. SVP Shared Services 2.SSP 3. Any Team member 4. EXECOM and MANCOM 5.HR 6.Building Admin 1. IT/SSP	Annual

		Theft during Fire		2. Maintain adequate fire suppression and fire alarm /detector equipment at strategic locations within the premises	2. Building Administrator	
				3. Depending on the extent of fire, conduct inventory of damage and salvageable equipment after occurrence of fire	3.Shared Services Team	
				4. Usage of Foam type fire extinguisher to minimize damage	4. SSP	
					1.IT	
				1. CP-IT-0501_V9_Network Services Acceptable Usage Policy 2. Insurance Claim	2. F&A/SSP	
Fire in the building	2	Injury to/Loss of Life of facility occupants	1	1. Assess extent of fire threat	1. SVP Shared Services	
	2		1	2. Notify PACSTAR building admin	2.SSP	
		Disruption of normal operations		3. Utilize fire suppression equipment to contain fire threat	3. Any Team member	
				4. Depending on fire threat, initiate facility evacuation procedures	4. EXECOM and MANCOM	Annual
	2		1	5. Where individuals have sustained injuries, administer first aid and coordinate with local emergency agencies once outside the facility	5.HR	
		Damage to Equipment		6. Conduct periodic fire drills	6.Building Admin	
				7. Implement CPP-HR-0404		
				1. Minimize damage thru power disconnection and system shutdown as deemed	1. IT/SSP	

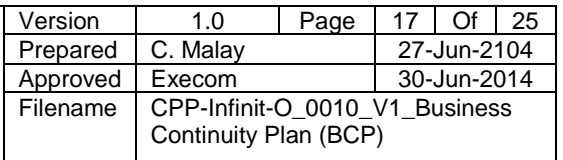|						
				necessary		
				2. Maintain adequate fire suppression and fire alarm /detector equipment at strategic locations within the premises	2. Building Administrator	
				3. Depending on the extent of fire, conduct inventory of damage and salvageable equipment after occurrence of fire	3.Shared Services Team	
				4. Usage of Foam type fire extinguisher to minimize damage	4. SSP	
Severe Typhoon or Flood	3	Disruption of normal operations due to lack of manpower	2	1. Monitor the weather advisory from local weather agency or news feeds. 2. Identify affected team 3. Mobilize pickup procedure.	1. MANCOM/ EXECOM: 2. SSP/MANCOM/ EXECOM 3. SSP/HR/MANCOM /EXECOM	Annual
Earthquake Intensity 1-4	1	Injury Damage to Equipment	1	1. Where individuals have sustained injuries, administer first aid and coordinate with local emergency agencies once outside the facility 2. Minimize damage thru power disconnection and system shutdown as deemed necessary 3. Maintain adequate fire suppression and fire alarm /detector equipment at strategic locations within the premises	1.HR 1. IT/SSP 2. Building Administrator 3.Shared Services Team	

	Company Policy & Procedure Manual **Business Continuity Plan (BCP)** Ref. No.: CPP-Infinit-O_0010	Version	1.0	Page	15	Of	25
		Prepared	C. Malay		27-Jun-2104		
		Approved	Execom		30-Jun-2014		
		Filename	CPP-Infinit-O_0010_V1_Business Continuity Plan (BCP)				

					4. Depending on the extent of fire, conduct inventory of damage and salvageable equipment after occurrence of fire	5. SSP	
					5. Usage of Foam type fire extinguisher to minimize damage		
Earthquake Intensity 5 and above	3	Injury	1		1. Where individuals have sustained injuries, administer first aid and coordinate with local emergency agencies once outside the facility	1.HR	Every Two Years
		Damage to Equipment			1. Minimize damage thru power disconnection and system shutdown as deemed necessary	1. IT/SSP	
					2. Maintain adequate fire suppression and fire alarm /detector equipment at strategic locations within the premises	2. Building Administrator	
					3. Depending on the extent of fire, conduct inventory of damage and salvageable equipment after occurrence of fire	3.Shared Services Team	
		Threat to life of team members			4. Usage of Foam type fire extinguisher to minimize damage	4. SSP	
					1. Initiate emergency evacuation procedures, refer to Appendix B Pacific Star House rules		
Civil Unrest	1	Unauthorize	1		1. Once unauthorized	1. Shared	Every Two Years

		d Personnel at Facility Premises				entry has been detected, secure and detain unauthorized person(s)	Services Team
					2.	Coordinate with building admin and Alert local law enforcement authorities	2. Shared Services Team
Failure of Facility due to natural catastrophe - Short Term (one-to-three day shutdown)	3 3	Disruption of normal operations Failure to meet commitments to customers	1 1	1. 2.		If projected restoration to normal facility operations is short-term, advise Executive Management, Production Management and Support Service Groups. Advise customers of the situation, including status of work in progress, potential delays and estimated time to restoration of normal operations.	Shared Services CSG -VPs	Every Two Years
Failure of Facility due to natural catastrophe - Medium-Term (one week to less than one month shutdown)	3 3	Disruption of normal operations Failure to meet commitments to customers	1 1	1. 2. 3.		If projected restoration to normal facility operations is medium-term, identify possible temporary relocation sites to house production. Assess impact on delivery commitments on projects housed in the facility. Initiate temporary transfer of equipment to support vital production functions to selected relocation site 5km away from the	Shared Services EXECOM Shared Services MANCOM CSG-GROUP	

				office.	CSG -VPs	
				4. Advise production personnel regarding start of production at temporary relocation site		
				5. Resume production operations.		
				6. Advise customers of the situation, including status of work in progress, potential delays and estimated time to restoration of normal operations.		

APPENDIX B

		Version	1.0	Page	18	Of	25

| Company Policy & Procedure Manual **Business Continuity Plan (BCP)** Ref. No.: CPP-Infinit-O_0010 | Version | 1.0 | Page | 18 | Of | 25 |

Company Policy & Procedure Manual
Business Continuity Plan (BCP)
Ref. No.: CPP-Infinit-O_0010

Version	1.0	Page	18	Of	25
Prepared	C. Malay		27-Jun-2104		
Approved	Execom		30-Jun-2014		
Filename	CPP-Infinit-O_0010_V1_Business Continuity Plan (BCP)				

BCP Testing and Results

1.0 The organizations BCP should be tested at least annually to ensure credible recovery and disaster preparedness.

2.0 EXECOM shall determine the scope of testing, the objectives, and measurement criteria of each test on a per event basis.

3.0 MANCOM, SSP, and IT teams will assist and coordinate in the testing of specified events as required by EXECOM.

SCENARIO	SCHEDULE	RESULTS	RCA/Corrective Actions
Power Failure (may be a result of Fire, Typhoon, Flooding or Earthquake, Building preventive maintenance)	April 17 – 18, 2014	Generators were rented to provide alternative power to teams in the office while PACSTAR power was turned off. The rented generators were unable to provide power to all teams. A solution was worked out by IT to temporarily transfer teams with no power to an area of the building that the generators could provide power to. A total of 2.5 hours downtime was accumulated by all affected teams. Some teams used this time to go on break.	Root Cause: Miscommunication on planned arrangement. Containment: IT temporarily transferred teams with no power to the area in the office that the generators could provide power to. Corrective Action: Involve building admin during planning.
Call Tree	May 26, 2014		
Fire	TBA	*PENDING FIRE DRILL OF PACIFIC STAR BUILDING*	
Earthquake	TBA	*PENDING FIRE DRILL OF PACIFIC STAR BUILDING*	
Severe Typhoon or Flood	July 2014		

	Company Policy & Procedure Manual **Business Continuity Plan (BCP)** Ref. No.: CPP-Infinit-O_0010	Version	1.0	Page	19	Of	25
		Prepared	C. Malay		27-Jun-2104		
		Approved	Execom		30-Jun-2014		
		Filename	CPP-Infinit-O_0010_V1_Business Continuity Plan (BCP)				

APPENDIX C

PPTS Matrix

1.0 No Internet Connection

Vulnerability	Timeline	Actions	Person Responsible	Reference / resources needed
People	n/a	n/a	n/a	n/a
Process and data	5 minutes	Ensure that any local data is saved in the local workstations or local file server. Data stored in the client server or in the cloud should not be affected as long as the auto save feature is enabled	Team members on duty	
	5 minutes	Asses if the disruption will affect deliverables for the project	MANCOM or Project Handlers	
	45 minutes	For projects whose delivery will be affected, contact the client point person via phone or through another channel (mobile phone/internet) and advise of the situation, including estimated time to restore(details should be acquired through IT team member on duty)	MANCOM	
	60 minutes	Asses which projects have to be relocated (e.g. time sensitive projects). Initiate the relocation plan.	MANCOM	Relocation Plan and Procedures
Technology and Infrastructure	1 minute	Report to the IT Support personnel on duty (ext 203 or in person).	Team member on duty	otrs@infinit-o.com dial ex 203 approach in person
	5 minutes	Ensure automatic fail-over to another ISP	IT team member on duty	IT team troubleshooting manual IT team procedures
	10 minutes	Manually route the network to the back-up line if automatic fail-over was not successful.	IT team on duty.	IT team troubleshooting manual Vendor directory (ISP) IT team procedures
	30 minutes	Start process for identification of potential cause of failure. If external, coordinate with ISP and acquire the estimated time to restore service. If internal, proceed with the troubleshooting steps in the IT support	IT team on duty	IT team troubleshooting manual Vendor directory (ISP) IT team procedures

		manuals.		
	40 minutes	Issue an advisory to all MANCOM and EXECOM members if downtime cannot be resolved in the first 30 minutes. Advisory should include preliminary findings/root cause, estimated time to restore, and any other containment actions based on the initial troubleshooting	IT team on duty	IT team troubleshooting manual Infinit-o directory
	120 minutes	Prepare the equipment for transport and setup in designated relocation area.	IT team on duty	If relocation plan and procedures is initiated
Security and Facility	>60 minutes	Ensure that the equipment is secured during transport.	IT team on duty	Relocation Plan and Procedures

2.0 Power Failure (May be a result of the following: Fire, Typhoon, Flooding or Earthquake)

Vulnerability	Timeline	Actions	Person Responsible	Reference / resources needed
People	n/a	n/a	n/a	n/a
Process and data	5 minutes	Ensure that any local data is saved in the local workstations or local file server. UPS are in place to ensure that there is enough time to save any local data. Data stored in the client server or in the cloud should not be affected as long as the auto-save feature is enabled.	Team members on duty.	
	5 minutes	Asses if disruption will affect deliverables for the project.	MANCOM members on duty	
	45 minutes	For projects whose delivery will be affected, contact the client point person via phone or through another channel (e.g. mobile phone and internet) and advise of the situation, including estimated time to restore (details should be acquired from the IT Team Member on Duty).	MANCOM members on duty	If power is not restored within 30 minutes and upon advisory from SSP. Client directory
	60 minutes	Asses which projects have to be relocated. Initiate relocation plan.	EXECOM members	Assessment from MANCOM and estimated restoration time from SSP.
Technology and Infrastructure	1 minute	Ensure that the following is set up to run for at least 120 minutes on battery/UPS back-up a. At least one server b. At least two workstations c. At least one phone line	IT team on duty	
	1 minute	Ensure all emergency lights are	SSP team on duty	

	Timeline	Actions	Person Responsible	Reference/resources
		functioning. Replace faulty ones.		
	5 minutes	Ensure that controls of Pacific Star engineering team are in play.	SSP and IT team on duty	
	30 minutes	Issue an advisory to all MANCOM and EXECOM members if downtime cannot be resolved in the first 30 minutes. Advisory should include preliminary findings/root cause, estimated time to restore and any other containment actions based on the initial troubleshooting.	SSP team on duty	
		Asses if projects will need to relocate. Identify projects in need of immediate relocation.	MANCOM	
	120 minutes	Prepare the equipment for transport and setup in the designated relocation area.	IT team on duty	
	12 hours / 24 hours	If power outage from the utility is not restored within 12 hours (even if generator is running), asses the need for relocation. Assessment will be done every 12 hours. Initiate relocation plan	EXECOM members	Assessment from MANCOM and estimated restoration time from SSP. Relocation plan and procedures
Security and Facility	n/a	Data security should not be affected	n/a	n/a
	5 minutes	Ensure that back-up power on all proximity door locks are working. If the main proximity doors are malfunctioning, report to SSP team on duty.	IT team member	Infinit-o directory *Note: Proximity door locks should be checked on a regular basis.*
	10 minutes	Request for security support from building security personnel on duty. Designated support team members should be manning the main facility entrance.	SSP team on duty	Upon advisory from the IT team member on duty. Vendor directory (building security /admin)
	>60 minutes	Ensure that equipment is secured during transport	IT team on duty	Relocation plan and procedures

4.0 Workstation or Server Problems

Vulnerability	Timeline	Actions	Person Responsible	Reference/resources needed
People	n/a	n/a	n/a	n/a
Process and Data	5 minutes	Ensure that any local data is saved in the local workstations or local file server. Data stored in the client server or in the cloud should not be affected as long as auto-save feature is enabled.	Team members on duty	
	5 minutes	Assess if the disruption will affect deliverables for the project.	MANCOM members on duty	Infinit-o directory
	45 minutes	For projects whose delivery will be affected, contact client point person via phone or another channel and advise of situation, including estimated time to restore. Details should be acquired from IT team member on duty	MANCOM members on duty	Client directory If issue is due to a file server problem, and upon advisory from SSP.
Technology and	1 minute	Report any workstation	Team member	

Infrastructure		performance issues to the IT team via ext 203 or otrs	affected	
	10 minutes	Perform troubleshooting steps as prescribed by the manual. Determine root cause of the problem.	IT team on duty	IT team troubleshooting manual
	30 minutes	If problem is due to a virus or malware: 1. Disconnect the affected workstation/server from network 2. Commence virus/malware cleanup 3. Disseminate the identification, containment and prevention information to everyone via email blast	IT team on duty	IT team troubleshooting manual Infinit-o company directory
	30 minutes	If problem is not due to a virus or malware (e.g. potential software or hardware issues, troubleshoot as prescribed by manual.	IT team on duty	IT team troubleshooting manual
	30 minutes	If problem affected the file server: 1. Identify any potentially affected or missing files. 2. Initiate the local data restoration process (data is backed up daily/weekly as per IT protocol). 3. IF the restoration process will take longer than 60 minutes, advise the team member / Mancom of the estimated time for completion.		IT team troubleshooting manual
	35 minutes	If issue was not resolved within 30 minutes (regardless of root cause), deploy spare workstation. As soon as the issue is fixed, re-deploy original workstation and pull out spare.	IT team on duty	IT team troubleshooting manual
Security and Facility	30 minutes	Ensure that there is no data security breach if the problem is due to malware/virus.	IT team on duty	IT team troubleshooting manual

5.0 Fire in the Building

Vulnerability	Timeline	Actions	Person Responsible	Reference/resources needed
People	1 minute	Attempt to contain fire using fire extinguishers Report any sign of fire to any MANCOM team member/admin on duty. Provide details as to where and description of affected area. Sound fire alarm if needed	Team member on duty	Fire extinguishers
	2 minutes	Assess extent of fire threat	SSP/MANCOM/EXECOM	Emergency directory

Company Policy & Procedure Manual
Business Continuity Plan (BCP)
Ref. No.: CPP-Infinit-O_0010

Prepared	C. Malay 27-Jun-2104
Approved	Execom 30-Jun-2014
Filename	CPP-Infinit-O_0010_V1_Business Continuity Plan (BCP)

Vulnerability	Timeline	Action	Person responsible	Reference
		Inform building administrator or fire department	member on duty	
		Utilize fire suppression equipment to contain fire threat	Team member on duty	Fire extinguishers
	5 minutes	If fire cannot be contained, initiate evacuation plan. Coordinate with Pacific Star Building Admin on evacuation plans	MANCOM team member on duty/designated team members.	1. Designated team member to ensure
	10 minutes	If there are team members who need medical attention: 1. Call medical emergency hotline 2. Conduct first aid as appropriate	MANCOM team member on duty/designated team members or HR team	Emergency directory (Medical dept.)
	>10 minutes	Seek clearance from the fire dept. before attempting to return to workplace	EXECOM/IT/SSP/MANCOM on duty	Emergency directory (fire dept.)
Process and Data	n/a	Data stored in the client server or in the cloud should not be affected as long as the auto-save feature is enabled		RISK: Data stored for the last 24 hours in the local workstations may be lost
	45 minutes	Asses if the disruption will affect deliverables for the project. Contact the client point person via phone or through another channel and advice of the situation.	MANCOM members on duty	Client directory
	60 minutes	Asses which projects have to be relocated (e.g. time sensitive projects) Initiate relocation plan	EXECOM members	Based on the project impact assessment from MANCOM and damage assessment from SSP
Technology and Infrastructure	5 minutes	Initiate IT evacuation plan 1. Carry pre-identified critical equipment (e.g. servers, mission critical workstations) 2. Team members who have been issued laptops should bring it with them during evacuation	IT team on duty	IT evacuation plan
	120 minutes	Prepare the equipment for transport and setup in the designated relocation area.	IT team on duty	Relocation plan and procedure IT evacuation plan
Security and Facility	30 minutes	Assess extent of the damage and estimated time to return to workplace.	SSP on duty	Emergency directory
	4 hours	If return to workplace cannot be guaranteed within 4 hours, initiate relocation plan	EXECOM members	Based on the damage assessment from MANCOM and estimated restoration time from SSP
	>60 minutes	Ensure that equipment is secured during transport.	IT team on duty	Relocation plan and procedures

6.0 Severe Typhoon or Flood

Vulnerability	Timeline	Action	Person responsible	Reference
People	n/a	n/a	n/a	n/a
	10 minutes and 30 minutes interval after	Monitor the weather advisory from the local	SSP on duty	LGU directory Infinit-o directory

	Company Policy & Procedure Manual	Version	1.0	Page	24	Of	25
	Business Continuity Plan (BCP)	Prepared	C. Malay		27-Jun-2104		
	Ref. No.: CPP-Infinit-O_0010	Approved	Execom		30-Jun-2014		
		Filename	CPP-Infinit-O_0010_V1_Business Continuity Plan (BCP)				

	the initial assessment	weather agency or LGU		
	10 minutes (from determination of danger)	Monitor the weather advisory from the local weather agency or LGU.	Designated EXECOM members	Infinit-o directory
	10 minutes (from determination of danger)	Identify potential teams that will be affected.	SSP/MANCOM/EXECOM	LGU directory Vendor directory (building admin)
	15 minutes (from determination of danger)	Initiate evacuation plan if there is a confirmed threat to building.	EXECOM	Evacuation plan (typhoon and flood)
		Mobilize pick up procedure if needed	EXECOM	
Process and Data	n/a	n/a	n/a	n/a
	10 minutes (from determination of danger)	Asses if disruption will affect deliverables of project.	MANCOM members on duty	
	45 minutes (from determination of danger)	Contact client point person via mobile phone or other channels and advise of situation including estimated time to restore (details should be acquired from IT team member)	MANCOM members on duty	Client directory
	60 minutes (from determination of danger)	Asses which projects have to be relocated. Initiate relocation plan.	EXECOM members	Relocation plan and procedures
Technology and Infrastructure	15 minutes (from determination of danger)	Initiate IT evacuation plan. 1. carry pre-identified critical equipment 2. laptops	IT team members on duty	IT evacuation plan
	120 minutes	Prepare equipment for transport and set up in designated relocation site	IT team members on duty	IT evacuation plan
Security and Facility	Every hour after evacuation	Assess extent of any damage and estimated time to return to workplace	SSP team member on duty	LGU directory Vendor directory (building admin)
	4 hours	IF return to workplace cannot be guaranteed within 4 hours initiate relocation plan	EXECOM team members	Relocation plan and procedure
	>4 hours	Ensure equipment is secured during transport	IT team	Relocation plan and procedures

7.0 Phone Problems

Vulnerability	Timeline	Action	Person responsible	Reference
People	n/a	n/a	n/a	n/a
Process and Data	5 minutes	Team member should use the secondary dialing procedure. OTRS for IT should have already been sent.	Team member and IT	
	10 minutes	Asses if disruption will affect deliverables of the project. IT to contact provider to get updates on disruption	MANCOM and IT	
	30 minutes	Assess which projects	EXECOM	

		have to be relocated.		
Technology and Infrastructure				
Security and Facility	n/a	n/a	n/a	n/a