Business Continuity Plan

Redback Operations

TABLE OF CONTENTS

CHANGE CONTROL

Document Control and Review

Document Control	
Author	Joel Daniel
Owner	Redback Operations - Cybersecurity
Date Created	22nd April 2024
Last Reviewed By	
Last Date Reviewed	
Approver and Date	
Next Review Date	

Version Control

Version	Date of Approval	Modified By	Approved By	Description of Change
0.1		Joel Daniel		Initial Draft
0.2		Joel Daniel		Set Appendices to Portrait format
0.3		Joel Daniel		Modified Backups, Appendices and Emergency Kits based on feedback.
1.0	13 May 2024	Joel Daniel	Ben Stephens	Approved for Publishing

1. INTRODUCTION

The Business Continuity Plan (BCP) will detail the actions to be taken to ensure that the company, REDBACK OPERATIONS, remains at minimal operational capacity to satisfy customer and production plans in the occurrence of various interruptions and events.

The document will dictate minimal actions ranging across a variety of scenarios, alongside general activities that need to be carried out pre and post scenario.

Note :- Please note that in-depth steps for assets and recovery will be detailed in the Redback Operations Disaster Recovery document, with only a surface level explanation described in this document.

2. SCOPE

The document is only scoped to the activities of Redback Operations as well as its assets (currently owned and expected). The document is only limited to the Geelong Waurn Ponds Campus environment in terms of physical activity.

3. STAKEHOLDERS

3.1 The following stakeholders (Company Board) will have a copy of the BCP at all times, and will operate as the authoritative figures for the company overall. These members will also operate as the **PRIMARY** communicative and responsive figures between the company and other parties such as the Capstone Companies and Deakin University, as well as coordination between the various members of the company. The authoritative hierarchy is detailed from highest to lowest in numerical order below.

1. Company Director = **Daniel Lai**
2. Company Mentors =
    - **Ben Stephens**
    - **Morgaine Barter**
    - **Ashish Manchanda**
    - **Fatimeh Ansarizadeh**
3. Company Leaders =
    - **Matt Hollington**
    - **Mehak**

3.2 The following stakeholders (Project Leaders) will have a copy of the BCP at all times, and will operate as the authoritative figures for each project/team in the company. These members will also operate as the primary communicative figures between the company board and leaders and the relevant projects. Project Sub team leaders will report to these stakeholders.

1. Project 1 (VR Suncycle & Smart Bike) = **Jai Watts**
2. Project 2 (Elderly Wearable Tech Sensors) = **Aman Kag**
3. Project 3 (Athlete Wearable Tech Sensors) = **Brendan Kay, Ojasvi Singh**
4. Project 4 (Crowd Monitoring & Player Tracking) = **Saksham Behal**
5. Data Warehousing = **Joel Daniel**
6. Cyber Security = **Joel Daniel**

Note :- Projects can change over the trimesters and the above is not an exhaustive list. Names above are as of Trimester 1 (June 30th) 2024.

4. EMERGENCY ESSENTIALS KIT

The Emergency Essentials Kit contains documents and content that provide information and credibility to the business' operations and incurred activities from external parties such as banks, suppliers etc….

Due to the operating and digital nature of Redback Operations, the Digital Kit should be prioritized at the project and company level, while the Physical Kit should be created only for projects where there will be vital physical artifacts.

4.1 Digital Kit

- Ensure that only authorized entities, who would be the company board, have access to the digital kit.
- It is recommended to have at least two digital kits stored in separate locations/servers/file paths that can be accessed over the Internet or an Intranet line.
    - Do note that saving the digital kit on removable storage media will count as a physical kit and thus adhere to the above section.
    - It is further recommended to store the digital kit on two separate cloud platforms (Google Drive and Microsoft OneDrive or any combination of equivalents) to further secure against vendor specific disruptions or accessibility issues.

4.2 Physical Kit

- Ensure that the bag/box used to contain the relevant essentials is waterproof, fireproof and tamperproof as much as possible.
- It is recommended to have at least three of these kits, stored in different locations and far away from each other, accessible to a member of the company board (preferably the mentors or leaders).
    - Project Leaders can have their own project-specific kits ready and distributed among their own members at their discretion.
- Ensure that the kit is secured from access by unauthorized entities, as these kits will contain sensitive information.
- Ensure a copy of physical artefacts (keys, ID cards etc….) are placed in the kit as required.

- However do note that artefacts that belong to extremely sensitive assets like administrators or central servers are to not be stored in the kit. Only the company board members may have these assets in a separate location.

4.3 Required Contents

The following items need to be present in the emergency essential kits that are prepared.

- Business Operational Plans for the Trimester (in this instance it would be Tasks 2.1P, 5.1P and 10.1P alongside the T3 equivalent).
- Employee Register and Board Grouping.
- Documents regarding loans from financial institutions and third-parties.
- Documents regarding agreements with suppliers and vendors.
- Documents regarding contracts (alongside project progress if possible) with clients.
- Documents regarding insurance of assets.
- All Company-wide Policies (Cyber Security, Incident Response, Business Continuity Plan, Disaster Recovery etc.…)
- Network and System Diagrams.
- Company Board and Leadership Contact Information.

Note :- The latest versions of the above as soon as possible need to be placed/updated in the kits.

5. DIGITAL BACKUPS, ASSET SPARES AND OTHER PROTECTION

This section will detail the relevant locations for the various digital backups, asset spares and parts that will be possessed by Redback Operations for redundancy and safekeeping, as well as any other protection and risk reduction mechanisms in place such as Insurance, Funds etc….

5.1 Digital Backups

Digital Backups are in regard to large scale backups such as Virtual Machines, Datasets, Applications, Storage etc…..and thus do not fall under Digital Emergency Kits (which only contain critical files).

Digital Backups need to adhere to the following requirements:

1. Backups need to be carried out on a timely basis as below:
    - Daily backups need to be made on-site prior to End of Day or immediately after End of Day if automated.
    - Weekly backups need to be made can placed off-site, recommended to be done at the end of the work week or the weekend if automated.
2. The backups need to follow the below types:
    - Daily Backups can be either Incremental or Differential Backups.
    - Weekly Backups need to be Full Backups.
3. Backups need to be stored securely in separate locations from the main environment, with no connection (digital or physical) to it.
    - *However, at the company board's discretion, ONLY ONE backup can be kept connected to the environment to facilitate quick recovery.*
4. At minimum there should be two backups, while adhering to the 2nd condition of this list.
    - *However, at the company board's discretion, projects can keep their own backups as well, be it full or incremental or differential or mirror at their own discretion.*
5. Only authorized entities (adhering ONLY to the Stakeholders section in this document) are allowed to access, modify or delete backups and their storage location. These actions taken should be documented.

Any and all backups, be it at the company level or project level, need to have their records stored in the Digital Backups table (Table 1) found in the Appendix.

5.2 Asset Spares

Asset Spares include full scale replicas of assets as well as spares at the parts level to replace and fix assets.

Asset Spares need to adhere to the following requirements:

1. Spares need to be routinely checked to ensure that no new replacements or fixing is required (ensure spares are maintained and in a ready-to-use state).
2. It is recommended to have at minimum in storage:
    a. ONE full replicas of large scale assets (smart bike)
    b. THREE replicas of small scale assets (sensors, watches etc.…)
    c. THREE spares of parts for building assets (circuit boards, frames etc…)
    d. TWO spares of tools
    e. ONE spares of large scale infrastructure (tables, saws etc…)

    However, at the company board's and project leader's discretion, the above number can be reduced to ONE at reasonable conditions.
3. One replica at minimum can be stored in the same location as that of the main used items (spare parts can be increased to 2-3 based on usage) and work environment. All other replicas and spares need to be stored in other secure locations away from the work environment.
4. Only authorized members (adhering to the Stakeholders section in this document AND authorized project members for each project specific item) are allowed to access the spares and the storage locations.

Any and all replicas and spares, be it at the company level or project level, need to have their records stored in the Asset Spares table (Table 2) found in the Appendix.

5.3 Insurance and Other

Insurance and Other relate to the various financial, support plans and partnerships that the company has to mitigate and reduce negative impact as well as support restoration of assets, infrastructure and company operations from minimal function to general operational capabilities.

Insurance and Other need to adhere to the following criteria:

1. Policies, plans and agreements need to reviewed and agreed upon by the board and project leaders every trimester.
2. The company board will have the final decision on any partnerships/policies/plans being placed into use.
    a. *However the company board MUST gain approval where required from the School of IT per Deakin regulations and procedures.*

Any and all policies/plans/partnerships, be it at the company level or project level, need to have their records stored in the Insurance and Other table (Table 3) found in the Appendix.

6. IMMEDIATE RESPONSE PLAN

When an incident occurs that activates this plan, ensure the following responses are carried out (while recommended to follow in order, the order can be voided at the discretion of the authoritative figures in the Stakeholders section).

1. Establish communications among Stakeholders affirming everyone in contact and safe.
    a. Project leaders do the same with their project teams and give Stakeholders a periodical update.
2. Check for injuries among company members and contact emergency services (see Emergency Contact List in Appendix) if required.
3. Assess severity of incident.
4. Assess accessibility and usability of company assets, environment and infrastructure.
    a. If required, evacuate the company working site and relocate to a safe location.
5. Ensure that an emergency essentials kit is accessible and currently in possession among the company board.
6. Check if company digital infrastructure and communication lines are active and accessible.
    a. If not, fall onto alternate lines and decided by the company board and project leaders.
7. Brief company on incident status and damage findings.
    a. Ensure that Deakin University and other relevant partners (Capstone Unit companies, School of IT etc.…) are in the loop.
8. Implement continuity actions for critical operations and assets in the company.
    a. Refer the Disaster Recovery Documentation for more information.

Please note that should the above responses not be feasible in a situation, actions the preserve and protect the SAFETY AND WELLBEING OF HUMAN (AND WHEN APPLICABLE ANIMAL) LIFE should be PRIORITIZED FIRST over any other actions.

6.1 Evacuation Procedures

As current company operating physical environments are within Deakin University premises, adhere to the Deakin evacuation plans.

For large scale natural disasters, government evacuation and response plans supersede initial response procedures.

7. CONTINUITY PLAN

Once company members are confirmed to be secure (or at minimum the primary points of contacts and operations to maintain minimal operations), the following actions are to be carried out to maintain operational capabilities at acceptable levels:

- Identify the critical/time-sensitive operations that are impacted and unable to operate at daily operational levels/output.
- If any non-impacted operations are functional, check the flexibility of members involved in other operations to temporarily assist in impacted operations.
    - *Members from other operations can be asked to assist only if necessary to maintain minimal operations.*
- Analyze impacted operations and determine the effort and resources it would take from what assets and access are available to maintain minimal operational capacity.
    - *Efforts to push beyond minimal capacity or even reach normal operational capacity should NOT be attempted during this time unless surplus assets and effort are available to assure no below minimal performance in case of issues.*
- Prioritize impacted operations that can be quickly restored to minimal operations and carry out the relevant actions.
    - *Order of impacted operations restoration to minimal operational capacity can be overridden by the company board at their discretion.*

For a detailed view of which operations are considered critical in nature, their RPO, RTO and MTD as well as relevant continuation actions can be found in Table 4 in the Appendix.

For detailed views on recovery of assets and operations after minimal operational capacity, refer the Disaster Recovery Plan.

8. REVIEW AND TRAINING

- Ensure that relevant evacuation plans and drills for physical locations and environments are executed for staff training once every trimester.
- While the BCP is for the stakeholder's possession, allow new staff members to have a read through the plan barring the appendix (they should not possess the plan, nor have access to sensitive information relevant to the plan).
- Review the BCP on a regular basis (recommend once a trimester for the stakeholders, but at minimum it should be done annually a year from the last update/review).
    - Changes done in this review include (but are not limited to) new procedures, updated sections etc….
    - *Note that the Appendix has to be kept updated as much as possible, and does not require a review time to be updated by authorized entities. Changes are not limited to but include:*
        - *Structural Organization change.*
        - *Change between partners.*
        - *Changes to projects (new projects or defunct projects).*
        - *Emergency Kits, Digital Kits and Backup storage updates.*

APPENDICES

Appendix A = Backups, Spares, Critical Business Operations and Others

Data for Backup	Affected Project	Responsible Person	Backup Frequency	Backup location	Backup type	Backup media
eg:- Athlete Dataset	Project 3	Brendan Kay	Weekly	Sharepoint (URL)	Full Backup	Digital DB File

Table 1: Digital Backups

Asset	Affected Project	Responsible Person	Nos of items	Storage Location
eg:- Smartbike	Project 1	Jai Watts	3	Deakin University Geelong - Level 1 Lab

Table 2: Asset Spares

Partner/Insurance	Support Type	Coverage	Any exclusions?	Company/Project	Payment Cost	Payment Frequency	Expiry/Review Date
eg:- Insurance XYZ	Asset Insurance	All physical assets	Not applicable to testing incidents	Company-wide	1000 AUD	Monthly	10th December 2024

Table 3: Insurance and Other

Business Operation	Description	Priority	Loss Impact	Continuity Steps	RPO	RTO	MTD
eg:- Firewall Defense	Firewalls providing network partitioning, access control and network protection	Critical	• Risk of unauthorized access into digital environment. • Project services locked out of network. • Potential shutdown of all traffic on network.	• Enable fail-open services for non-critical activities. • Attempt direct access to firewalls with main administrator credentials. • Establish minimal network paths for minimal vital company operations requirements.	12 hours	24 hours	36 hours

Table 4: Critical Business Operations

- *RPO (Recovery Point Objective) = The maximum duration of data loss that can be accepted before incident.*
- *RTO (Recovery Time Objective) = The time after incident within which the operation has to be brought back to minimal operational capacity.*
- *MTD (Maximum Tolerable Downtime) = The maximum time since incident at which an operation can stay out of operation before any significant negative impact.*

Appendix B = Organization and Emergency Contacts

Name	Company Role	Mobile Contact	Email	Responsibilities in Emergency	Has Emergency Essentials Kit?	Has Digital Kit?
Matt Hollington	Leader	0xxx xxx xxx	s222348917@deakin.edu.au	• First Point of Contact for decision-making and notifications. • Chief Officer in activating BCP and DR responses. • Primary contact for acquiring emergency resources and services. • Primary contact for communications between team leaders and company board.	Yes	Yes
Mehak	Co-Leader	0xxx xxx xxx	s222194342@deakin.edu.au	• First Point of Contact for decision-making and notifications. • Chief Officer in activating BCP and DR responses. • Primary contact for acquiring emergency resources and services. • Primary contact for communications between team leaders and company board.	Yes	Yes

Morgaine Barter	Mentor	0xxx xxx xxx	morgaine.barter@deakin.edu.au	• Secondary Point of Contact (should Primaries fail to respond) for decision-making and notifications. • Primary contact for communications between company board and Deakin staff & security. • Secondary contact for communications between team leaders and company board. • Primary contact for enacting secondary actions such as Disaster Recovery, Asset Recovery etc…	Yes	Yes
Ben Stephens	Mentor	0xxx xxx xxx	ben.stephens@deakin.edu.au	• Secondary Point of Contact (should Primaries fail to respond) for decision-making and notifications. • Primary contact for communications between company board and Deakin staff & security. • Secondary contact for communications between team leaders and company board. • Primary contact for enacting secondary actions such as Disaster Recovery, Asset Recovery etc…	Yes	Yes
Daniel Lai	Director	0xxx xxx xxx	daniel.lai@deakin.edu.au	• Coordinate communications in regards to information updates and decisions between Redback Operations and Deakin University/Government Entities/Partners	Yes	Yes

Table 5: Redback Operations Stakeholders Details

Emergency Service Contacts	Contact Number	Address (closest)
Police		
Ambulance		
Hospital		
Medical		
Deakin Security		
Electrical		
IT Support		
Water		
Gas		
Partner Contacts	**Contact Number**	**Address**
eg:- Hardware Bikes Pvt		

Table 6: Emergency and Partner Contact Details