
# Disaster Recovery Document

Redback Operations
Cyber Security Team

# Contents

## Document Control and Review

| Document Control | |
|---|---|
| Author | Liam Fern & Surekha Kanagasingam |
| Owner | Redback Operations - Cybersecurity |
| Date Created | 6th May 2024 |
| Last Reviewed By | Joel Daniel |
| Last Date Reviewed | 10th May 2024 |
| Approver and Date | Joel Daniel – 10th May 2024 |
| Next Review Date | 7th March 2025 |

### Version Control

| Version | Date of Approval | Modified By | Approved By | Description of Change |
|---|---|---|---|---|
| 0.1 | | Liam Fern & Surekha Kanagasingam | | Initial Draft |
| 1.0 | 10th May 2024 | Liam Fern & Surekha Kanagasingam | Joel Daniel | Approved for Publishing |

## Overview

This Disaster Recovery Plan (DR Plan) provides an operational handbook for recovering data and systems critical to Redback Operations' operation.

In case of disaster resulting in data loss or access to any assets/platforms or systems used by Redback Operations, this document should be consulted, and the relevant recovery plan should be actioned.

This plan will cover recovering all critical assets and platforms Redback Operations uses. We aim to guarantee business continuity, data availability and integrity, and information system uptime.

The objectives of this plan are the following:

- To minimize interruptions to the normal operations.
- To limit the extent of disruption and damage.
- To minimize the economic impact of the interruption.
- To establish alternative means of operation in advance.
- To train personnel with emergency procedures.
- To provide for smooth and rapid restoration of service.

## Policy Owners

This policy is owned by the company board, including directors, mentors, and leaders.

Company Board as of Trimester 1 2024

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

## Key Personnel

Team Leaders must have a copy of this policy as they will act as disaster recovery team leads for their respective projects. A Company Leader or Mentor will be chosen to recover assets owned by Redback Operations as disaster recovery team lead.

| Name | Position | Address | Telephone |
|---|---|---|---|
| Jai Watts | Project 1 (VR Suncycle & Smart Bike) Lead | [Company Address] | [Contact Number] |
| Aman Kag | Project 2 (Elderly Wearable Tech Sensors) Lead | [Company Address] | [Contact Number] |
| Brendan Kay, Ojasvi Singh | Project 3 (Athlete Wearable Tech Sensors) Lead | [Company Address] | [Contact Number] |
| Saksham Behal | Project 4 (Crowd Monitoring & Player Tracking) Lead | [Company Address] | [Contact Number] |
| Joel Daniel | Data Warehousing/Cyber Security Lead | [Company Address] | [Contact Number] |

Table 1: Team Leaders as of Trimester 1 2024

## Assets Covered in this Plan

| Asset/Platform | Team |
|---|---|
| Google Cloud Platform | Redback Operations |
| On-premise Virtual Machine | Redback Operations |
| Smart Bike | Project 1 |
| Sensors | Project 2, Project 3 |

Table 2: Assets

## General Disaster Recovery Procedures

Upon discovering any disaster resulting in data loss or access to the assets defined in this document, the following disaster recovery initiation procedure should immediately commence.

1. Notify Company Leaders
2. The Disaster Recovery Lead is assigned to the relevant asset owner.
3. Disaster Recovery Lead to set up a disaster recovery team comprised of relevant stakeholders and representatives from their project/team
4. Disaster Recovery Team to determine the scope and degree of disaster, including
    a. Assets/Systems Affected
    b. Data Lost
    c. Time of Disaster
5. The Disaster Recovery Lead will distribute the disaster recovery plan to all team members.

## Application Profile

This section documents all critical software applications used by Redback Operations.

| Application Name | Critical? | Fixed Asset? | Manufacturer | Comments |
|---|---|---|---|---|
| UNITY | Yes | No | Unity Technologies | 1. Runs daily |
| Firebase | Yes | No | Google | 1. Runs daily |
| Microsoft Planner | Yes | No | Atlassian | 2. Runs weekly on Monday |
| Google Cloud Platform | Yes | No | Google | 1. Runs daily |

Table 3: Critical Applications

### Comment Legend:

1. Runs daily.
2. Runs weekly on [Day].
3. Runs monthly on [Day].

## Inventory Profile

This section comprises the list of hardware devices used by Redback Operations. It includes the following inventory:

- **Processing units**: Main servers for data processing.

- **Disk units**: Storage units for backups and data.
- **Models**: Specific hardware models in use.
- **Workstation controllers**: Controllers for managing multiple workstations.
- **Personal computers**: Computers assigned to employees.
- **Spare workstations**: Backup workstations for emergency use.
- **Telephones**: Office telecommunication devices.
- **Air conditioners or heaters**: Climate control units in server rooms.
- **System printers**: Printers used for office documentation.
- **USB Devicesand diskette units**: Backup storage media.
- **Controllers, I/O processors**: For managing inputs/outputs in network systems.
- **General data communication equipment**: Routers, switches.
- **Spare displays, racks**: Additional hardware components.
- **Humidifiers or dehumidifiers**: Environmental control in critical areas.

| Manufacturer | Description | Model | Serial No. | Owned/Leased | Cost |
|---|---|---|---|---|---|
| Dell | Processing Unit Server | PowerEdge T30 | 987654321 | Owned | $2054 |
| Dell | Backup Server | PowerEdge R450 Rack Server | 321231234 | Owned | $6500 |
| Seagate | Disk Unit | Expansion 5TB | 123456789 | Leased | $300 |
| HP | System Printer | ENVY Inspire 7920e | 564738291 | Owned | $151 |
| Cisco | Router | 4000 Series | 234567890 | Owned | $7000 |
| Cisco | Switch | Catalyst 9300 Series | 123131231 | Owned | $4000 |
| Lenovo | Personal Computer | ThinkCentre M720q | 345678901 | Owned | $700 |
| INVT | Air Conditioner | Rack Precision Cooling System | 456789012 | Owned | $50000 |
| Kesnos | Dehumidifier | 120 Pints Energy Star Home | 678901234 | Owned | $500 |

Table 4: Inventory Table of Hardware Devices

### Miscellaneous Inventory

This section includes additional essential non-fixed assets used in daily operations but not included in the main inventory:

| Description | Quantity | Comments |
|---|---|---|
| USB Devices | 100 | Used for offsite data backup. |
| COBOL Development Kits | 5 | Language software for legacy systems. |
| Printer Paper | 500 reams | Essential for printing project documents. |
| Windows OS | 100 | Required to perform day-to-day activities. |

Table 5: Inventory Table of Miscellaneous Inventory

## Information services backup procedures

- Backup Server
    - Daily, journal receivers are changed at 6:00 AM and at 6:00 PM.
    - Daily, a save of changed objects in the following libraries and directories is done at 1:00 AM:
        1. LIB_ACCOUNTING
        2. LIB_HR
        3. DIR_PAYROLL
        4. DIR_OPERATIONS
        5. LIB_SALES
        6. LIB_MARKETING
        7. DIR_SUPPORT
        8. LIB_IT

    This procedure also saves the journals and journal receivers.

    - On Sunday at 4:30 AM a complete save of the system is done.
    - All save media is stored off-site in a vault at SafeDataStorage, located in Melbourne.
- Personal Computer
    - It is recommended that all personal computers be backed up. Copies of the personal computer files should be uploaded to the server on every Friday at 5:00 PM, just before a complete save of the system is done. It is then saved with the normal system save procedure. This provides for a more secure backup of personal computer-related systems where a local area disaster could wipe out important personal computer systems.

# Disaster Recovery Procedures

## Emergency Response Procedures

Emergency response aims primarily at saving lives and reducing destruction caused by fire, natural disaster or other critical incidents. The following are immediate activities:

- **Evacuation Procedures:** Clearly identified exits and the way to evacuate. Regular practices should be done to ensure that all staff members know evacuation procedures.
- **Emergency Services Notification:** Immediate contact with fire, medical or police services is necessary when required.
- **Emergency Command Center:** A command center either on-site or nearby for coordinating the emergency response has to be set up.

## Recovery Actions Procedures

These procedures are essential in preserving the necessary data processing operational tasks that enable them to continue with minimal interruptions:

- **Data Backup:** Regular backups of all important data should be made and stored in a remote site. These back-ups go through regular tests so that they can be restored if need arises.
- **Cloud Services:** Access to applications and information from cloud computing resources should be maintained remotely.
- **Alternate Processing Facility:** A third-party facility agreement or mobile site use for business continuity.

These are the steps to take in order to recover data processing systems quickly after a disaster:

- **Assessment and Evaluation:** Evaluate what happened in terms of its impact on data processing systems.
- **Restoration Plan**: Put into effect a well-structured plan to restore hardware, software, and data from backups.
- **Testing:** After restoration, confirm that all the systems have been restored back to normal functioning again including security wise.

# Disaster Action Checklist

## Plan Initiation

1. **Notify Senior Management:** Immediately inform senior management about the occurrence of the disaster.
2. **Setup Disaster Recovery Team:** Communicate with and assign roles for members of the disaster recovery team.
3. **Degree of Disaster:** Find out how much extent and effect has this calamity had on Firm operations.
4. **Application Recovery Plan:** This should be done based on the magnitude of damage it has caused with continuous monitoring as required.
5. **Backup Site Coordination:** Fix timing and coordination with an alternative site which will host IT department should things go worse at current location?
6. **Vendor and Personnel Contact:** All hardware/software vendors who are needed must be notified as well as all other employees involved.
7. **Service Disruption Notification:** Users need to know when they can expect service interruptions to occur or how long these may continue for.

## Follow-Up Checklist

1. **Logistics and Supplies:** make arrangements for any cash emergency, transport means, accommodation and food services that may be necessary.
2. **Communication Setup:** Verify that all team members have all contact info and create a user participation plan.
3. **Office Setup**: In case of an emergency arrange for backup office supplies, rent or purchase necessary equipment and manage mail in/out deliveries.
4. **Operational Setup:** Establish the order in which applications will be run; determine workstations and offline equipment requirements; check forms needed for each application to confirm they are operational.
5. **Preparation for Movement:** Make sure everything is checked before it is moved to the backup site. This includes taking inventory of all data and equipment. Plan for additional item transportation.
6. **Documentation & Maps:** Generate multiple copies of every system or operational documentation, procedural manuals, as well as directions how to reach the backup location.
7. **Insurance notification:** Inform insurance companies about the accident so that processing claims can begin.

## Recovery Start-Up Procedures

1. **Disaster recovery services notification:** Getting in touch with disaster recovery services on chosen recovery plan. The countdown begins when notice is received at guaranteed delivery time.
2. **24/7 contact availability** – Furnish Disaster Recovery Services with a delivery point address where equipment could be taken along with contacts and alternate contacts available round-the-clock.

## Recovery plan-mobile site

1. Notify the Disaster Recovery Team Lead of the nature of the disaster and the need to select the mobile site plan.

2. Confirm in writing the substance of the telephone notification to the Disaster Recovery Team Lead within 48 hours of the telephone notification.

3. Confirm all needed backup media are available to load the backup machine.

4. Prepare a purchase order to cover the use of backup equipment.

5. Notify the facilities manager of plans for a trailer and its placement

6. Depending on communication needs, notify telephone company Telstra of possible emergency line changes.

7. Begin setting up power and communications at the mobile site.

a. Power and communications are prearranged to hook into when trailer arrives.

b. At the point where telephone lines come into the building at the central junction, break the current linkage to the administration controllers. These lines are rerouted to lines going to the mobile site. They are linked to modems at the mobile site.

c. This action could conceivably require Teleco Inc. to redirect lines at the central complex to a more secure area in case of disaster.

8. When the trailer arrives, plug into power and do necessary checks.

9. Plug into the communications lines and do necessary checks.

10. Begin loading system from backups.

11. Begin normal operations as soon as possible:

a. Execute daily jobs as scheduled.

b. Perform daily saves to ensure no data is lost during the recovery phase.

c. Conduct weekly saves as part of the ongoing data protection strategy.

12. Plan a schedule to back up the system in order to restore it on a home-base computer when a permanent site is available. Continue using regular system backup procedures to maintain data integrity.

13. Secure mobile site and distribute keys as required.

14. Keep a maintenance log on mobile equipment.

## Recovery plan-hot site

The disaster recovery service provides an alternate hot site. The site has a backup system for temporary use while the home site is being reestablished.

1. Notify the Disaster Recovery Coordinator of the nature of the disaster and of its desire for a hot site.
2. Request air shipment of modems to the hot site for communications.
3. Confirm in writing the telephone notification to the Disaster Recovery Coordinator within 48 hours of the telephone notification.

4. Begin making necessary travel arrangements to the site for the operations team.
5. Confirm that all needed USB Devices are available and packed for shipment to restore on the backup system.
6. Prepare a purchase order to cover the use of the backup system.
7. Review the checklist for all necessary materials before departing to the hot site.
8. Make sure that the disaster recovery team at the disaster site has the necessary information to begin restoring the site.
9. Provide for travel expenses (cash advance).
10. After arriving at the hot site, contact home base to establish communications procedures.
11. Review materials brought to the hot site for completeness.
12. Begin loading the system from the save USB Devices.
13. Begin normal operations as soon as possible:
    a. Daily jobs
    b. Daily saves
    c. Weekly saves
14. Plan the schedule to back up the hot-site system in order to restore on the home-base computer.

## Restoring the entire system

To get your system back to the way it was before the disaster, use the procedures on recovering after a complete system loss in the *Backup and Recovery*

*Before You Begin:* Find the following USB Devices, equipment, and information from the on-site USB Devicesvault or the off-site storage location:

- If you install from the alternate installation device, you need both your USB Devices media and the CD-ROM media containing the Licensed Internal Code.
- All USB Devices from the most recent complete save operation
- The most recent USB Devices from saving security data (SAVSECDTA or SAVSYS)
- The most recent USB Devices from saving your configuration, if necessary
- All USB Devices containing journals and journal receivers saved since the most recent daily save operation
- All USB Devices from the most recent daily save operation
- PTF list (stored with the most recent complete save USB Devices, weekly save USB Devices, or both)
- USB Deviceslist from most recent complete save operation
- USB Deviceslist from most recent weekly save operation
- USB Deviceslist from daily saves
- History log from the most recent complete save operation
- History log from the most recent weekly save operation
- History log from the daily save operations
- The *Software Installation* book
- The *Backup and Recovery* book
- Telephone directory
- Modem manual
- Tool kit

## Rebuilding process

The management team must assess the damage and begin the reconstruction of a new data center.

If the original site must be restored or replaced, the following are some of the factors to consider:

- What is the projected availability of all needed computer equipment?
- Will it be more effective and efficient to upgrade the computer systems with newer equipment?
- What is the estimated time needed for repairs or construction of the data site?
- Is there an alternative site that more readily could be upgraded for computer purposes?

Once the decision to rebuild the data center has been made, go to Disaster site rebuilding section.

## Testing the disaster recovery plan

Frequent evaluation and adjustment of operation procedures to suit the shifting data processing systems within the organization is a vital step in implementing and carrying out trial runs on Redback Operation's disaster recovery plan. This continuous process guarantees that the DR plan is up-to-date and efficient. Here are the systematic lists used to conduct recovery tests and detect areas where critical testing should be done as part of a DRP.

| Item | Yes | No | Applicable | Not Applicable | Comments |
|---|---|---|---|---|---|
| Select the purpose of the test. What aspects of the plan are being evaluated? | | | Applicable | | Trial recovery system from offsite backup. |
| Describe the objectives of the test. How will you measure successful achievement of the objectives? | | | Applicable | | Objectives include full system restoration within 4 hours and minimal data loss. |
| Meet with management and explain the test and objectives. Gain their agreement and support. | Yes | | | | Management has been informed and is ready to support the planned downtime for testing |
| Have management announce the test and the expected completion time. | Yes | | | | The test will be carried out on the next Saturday between 2 AM and 6 AM after it was announced. |
| Collect test results at the end of the test period. | | | Applicable | | Results should be recorded and studied too. |
| Evaluate results. Was recovery successful? Why or why not? | | | Applicable | | Assessment to be made based on recovery time as |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | well as integrity post-recovery of data. |
| Determine the implications of the test results. Does successful recovery in a simple case imply successful recovery for all critical jobs in the tolerable outage period? | | | Applicable | | To be discussed during follow-up meeting. |
| Make recommendations for changes. Call for responses by a given date. | | | Applicable | | Recommendations for any required adjustments before next month should be made as well. |
| Notify other areas of results. Include users and auditors. | Yes | | | | There is a plan to share findings widely while at the same time collecting responses from people about them also. |
| Change the disaster recovery plan manual as necessary. | | | Applicable | | Changes will be effected basing on test outcomes in addition to feedback given. |

Table 6: Conducting a Recovery Test

| Item | Yes | No | Applicable | Not Applicable | Comments |
|---|---|---|---|---|---|
| Recovery of individual application systems by using files and documentation stored off-site. | | | Applicable | | Very important in ensuring independent restoration of all apps. |
| Reloading of system tapes and performing an IPL by using files and documentation stored off-site. | | | Applicable | | This is a basic exercise that demonstrates whether or not systems can be restored. |
| Ability to process on a different computer. | | | Applicable | | If primary systems fail, this becomes an essentiality for business continuity purposes. |
| Ability of management to determine priority of systems with limited processing. | Yes | | | | It tests management decision making under resource constraints. |

| | | | | | |
|---|---|---|---|---|---|
| Ability to recover and process successfully without key people. | | | Applicable | | Robustness of the system should also be tested alongside clarity in documentation procedures. |
| Ability of the plan to clarify areas of responsibility and the chain of command. | Yes | | | | During crisis situations orderly mannerliness must always prevail hence its criticality . |
| Effectiveness of security measures and security bypass procedures during the recovery period. | | | Applicable | | Security protocols need to remain effective even in DR scenarios so verify that they still do work as expected. |
| Ability to accomplish emergency evacuation and basic first-aid responses. | Yes | | | | Safety procedures ought to be effective as well as adequately practiced upon while here. |
| Ability of users of real-time systems to cope with a temporary loss of on-line information. | | | Applicable | | Adaptability by users together with effectiveness exhibited by temporary solutions shall therefore serve as measures too. |
| Ability of users to continue day-to-day operations without applications or jobs that are considered noncritical. | | | Applicable | | Evaluate the functioning relationship between critical and noncritical systems. |
| Ability to contact the key people or their designated alternates quickly. | Yes | | | | Examine how well communication works and where it can be improved in an emergency. |
| Ability of data entry personnel to provide the input to critical systems using alternate sites and different input media. | | | Applicable | | Evaluate logistical support for remote operations |
| Availability of peripheral equipment and processing, such as printers and scanners. | | | Applicable | | Ensure that all the necessary hardware is working and available. |
| Availability of support equipment, such as air conditioners and dehumidifiers. | | | Applicable | | Check if environmental controls work under DR conditions. |
| Availability of support: supplies, transportation, communication. | Yes | | | | This is important to ensure recovery efforts continue without interruption |
| Distribution of output produced at the recovery site. | | | Applicable | | Verify data handling and output distribution in DR mode |
| Availability of important forms and paper stock. | | | Applicable | | This is necessary to ensure paper-based operations can continue uninterrupted |

| | | | | | |
|---|---|---|---|---|---|
| Ability to adapt plan to lesser disasters. | Yes | | | | Test the flexibility and scalability of the DR plan. |

## Risk Matrix

| Asset | Issue | Risk Matrix | | | Responsive Actions | Preventive Actions | Contingency Actions |
|---|---|---|---|---|---|---|---|
| | | Likelihood | Impact | Risk | | | |
| Google Cloud Platform | No Accessibility (to entire platform) | | | | 1. Inform company board of issue.<br>2. Attempt to leverage Deakin hosted datacenters/servers.<br>3. Initiate Local Machine Solutions.<br>4. Establish communications with Google Support. | NA | • Have local solutions (compute and storage) ready for deployment and use |
| | | | | | | | |
| | Temporary Platform Unavailability | | | | 1. Inform company board of issue.<br>2. Attempt to leverage Deakin hosted datacenters/servers.<br>3. Initiate Local Machine Solutions.<br>4. Establish communications with Google Support. | • Establish procedures for adding and removing users from company environment access.<br>• Ensure administrators have secure access and identities are secured. | • Have local solutions (compute and storage) ready for deployment and use |
| | | | | | | | |

| Asset | Issue | Risk Matrix | | | Responsive Actions | Preventive Actions | Contingency Actions |
|---|---|---|---|---|---|---|---|
| | | Likelihood | Impact | Risk | | | |
| | Storage Solution Deletion | | | | 1. Inform Project Lead.<br>2. Check for backups.<br>3. Attempt restoration of solution.<br>4. If restoration not possible, pivot to alternative solution (backup, local storage etc…)<br>5. Ensure that applications/visualizations dependent on solution are operational<br>6. Update company board. | • Ensure only authorised members have relevant read/write/execute access to storage solutions.<br>• Monitor activities of project members when dealing with infrastructure management. | • Have backup policies and solutions (cloud or local) available.<br>• Run backup activities periodically.<br>• Deploy coding for storage solution dependant applications to allow for quick and seamless pivoting to alternative storage solutions. |
| | | | | | | | |
| | Virtual Machine Deletion | | | | 1. Inform Project Lead.<br>2. Attempt restoration of solution.<br>3. Monitor performance of any VM-dependant applications/services.<br>4. Update company board.<br>5. Carry out recreation of virtual machine (from ground up or template). | • Ensure only authorised members have relevant read/write/execute access to virtual machines.<br>• Monitor activities of project members when dealing with infrastructure management. | • Have backup policies for virtual machines active.<br>• Have templates of created virtual machines stored for quick deployment.<br>• Have procedures set for creating and deploying virtual machines (device specifications etc…) |
| | | | | | | | |

| Asset | Issue | Risk Matrix | | | Responsive Actions | Preventive Actions | Contingency Actions |
|---|---|---|---|---|---|---|---|
| | | Likelihood | Impact | Risk | | | |
| | Firewall Access Block | | | | 1. Inform relevant project cloud administrator.<br>2. Review past actions carried out on firewall.<br>3. Ensure only administrative access to firewall.<br>4. Rollback changes made once authorized.<br>5. Test and ensure authorized access is available. | • Establish procedures for submitting requests to grant/revoke access through firewalls (whitelist/blacklist).<br>• Regularly check for security issues with firewalls (vulnerability patches, denial-of-service attacks etc….) and take appropriate actions.<br>• Ensure firewalls are updated to the latest versions as soon as possible. | • Have a previous blacklist/whitelist to replace the existing list if the list is identified as the issue.<br>• Ensure an administrator has access to rollback changes made to firewall.<br>• While its recommended that firewalls fail-close in times of error, for non-critical resources (at the relevant owner's discretion unless decided against), firewalls can be allowed to fail-open. |
| | | | | | | | |
| | | | | | | | |

| Asset | Issue | Risk Matrix | | | Responsive Actions | Preventive Actions | Contingency Actions |
|---|---|---|---|---|---|---|---|
| | | Likelihood | Impact | Risk | | | |
| On-Premise Virtual Machine | No Accessibility | | | | 1. Inform company board of issue.<br>2. Initiate Local Machine Solutions.<br>3. Establish communications with Deakin IT Support for troubleshooting. | • Have one or more additional virtual machines on-premise with backups.<br>• Inform and get permission from company board and project leads ahead of time if any updates or VM modifications that can impact the VM (shutdown, reboot, system-wide update etc….) is to be carried out.<br>• Limit number of users with elevated privileges (administrative) access on the VM. | • Have local solutions (compute and storage) ready for deployment and use |
| | | | | | | | |
| | Temporary Platform Unavailability | | | | 1. Inform company board of issue.<br>2. Initiate Local Machine Solutions.<br>3. Establish communications with Deakin IT Support for troubleshooting. | • Have one or more additional virtual machines on-premise with backups.<br>• Inform and get permission from company board and project leads ahead of time if any updates or VM modifications that can impact the VM (shutdown, reboot, system-wide update etc….) is to be carried out.<br>• Limit number of users | • Have local solutions (compute and storage) ready for deployment and use |

| Asset | Issue | Risk Matrix | | | Responsive Actions | Preventive Actions | Contingency Actions |
|---|---|---|---|---|---|---|---|
| | | Likelihood | Impact | Risk | | | |
| | | | | | | with elevated privileges (administrative) access on the VM. | |
| | | | | | | | |
| | Project-specific Clash | | | | 1. Inform affected project's leadership as soon as possible.<br>2. Attempt to temporarily rollback changes made to restore normal operability and troubleshooting. | • Inform and get permission from company board and project leads ahead of time if any updates or VM modifications that can impact the VM (shutdown, reboot, system-wide update etc….) is to be carried out.<br>• Limit number of users with elevated privileges (administrative) access on the VM. | • Have local solutions (compute and storage) ready for deployment and use |
| | | | | | | | |
| | | | | | | | |
| Microsoft Planner | No Accessibility (to entire platform) | | | | 1. Inform company leadership.<br>2. Project Leaders check for administrative access. | NA | • Utilize Microsoft Planner boards as a backup source.<br>• Ensure only authorized entities |

| Asset | Issue | Risk Matrix | | | Responsive Actions | Preventive Actions | Contingency Actions |
|---|---|---|---|---|---|---|---|
| | | Likelihood | Impact | Risk | | | |
| | | | | | 3. Move to alternate/local task boards | | have the relevant permissions to add/remove members and boards. |
| | | | | | | | |
| | | | | | | | |
| Smart Bike | Damaged product (fixable) | | | | 1. Move bike to secure location.<br>2. Assess damage to bike.<br>3. Assess time for basic project usability of bike.<br>4. Retrieve parts for restoring bike.<br>5. Take inventory of used parts and current status. | • Discuss and accept potential level of damage asset is allowed to take prior to any modifications/tests/uses.<br>• Attempt to carry out uses of asset which could result only in negligible to no damage unless recommendation above is agreed.<br>• Attempt to carry out repairs wherever feasible for damaged sections of asset as soon as possible prior to use.<br>• Ensure location of storage and work environment is secure and safe as much as possible from disasters (natural and man-made) | • Have enough spare parts and materials on standby to access and repair asset.<br>• Have a backup asset placed in a secure location for use while main asset is being repaired. |
| | | | | | | | |

| Asset | Issue | Risk Matrix | | | Responsive Actions | Preventive Actions | Contingency Actions |
|---|---|---|---|---|---|---|---|
| | | Likelihood | Impact | Risk | | | |
| | Damaged product (write off) | | | | 1. Inform project leader of loss of asset.<br>2. Inform company board and leadership team.<br>3. Dispose of asset (salvage parts if possible).<br>4. Retrieve/Purchase new asset.<br>5. Document issue and actions taken. | • Discuss and accept potential level of damage asset is allowed to take prior to any modifications/tests/uses.<br>• Attempt to carry out uses of asset which could result only in negligible to no damage unless recommendation above is agreed.<br>• Attempt to carry out repairs wherever feasible for damaged sections of asset as soon as possible prior to use.<br>• Ensure location of storage and work environment is secure and safe as much as possible from disasters (natural and man-made) | • Have a backup asset placed in a secure location for immediate use.<br>• Attempt to salvage written-off asset for parts or recuperation of finances if possible. |
| | | | | | | | |
| | Missing product (lost/stolen) | | | | 1.Inform project leader of loss of asset.<br>2.Ensure other assets are secure.<br>3.Inform person in charge of company purchases.<br>4.Retrieve replacement of asset (backup or purchase). | • Ensure that the asset is accessible only to authorized members in authorized locations and times (project-specific).<br>• Ensure storage location of asset is secure from unauthorized entry. | • Have a backup asset placed in a secure location for use while main asset is missing.<br>• (if possible) Have templates and spare parts to quickly recreate replica of |

| Asset | Issue | Risk Matrix | | | Responsive Actions | Preventive Actions | Contingency Actions |
|---|---|---|---|---|---|---|---|
| | | Likelihood | Impact | Risk | | | |
| | | | | | 5.Carry out relevant actions to ensure replacement is operational and secure. | | missing asset.<br>• Have enough spare parts and materials on standby to access and repair missing asset if located. |
| | | | | | | | |
| | | | | | | | |
| Sensors | Damaged product (fixable) | | | | 1. Move sensors to secure location.<br>2. Assess damage to sensors.<br>3. Assess time for basic project usability of sensors.<br>4. Retrieve parts for restoring sensors.<br>5. Take inventory of used parts and current status. | • Discuss and accept potential level of damage asset is allowed to take prior to any modifications/tests/uses.<br>• Attempt to carry out uses of asset which could result only in negligible to no damage unless recommendation above is agreed.<br>• Attempt to carry out repairs wherever feasible for damaged sections of asset as soon as possible prior to use.<br>• Ensure location of storage and work environment is secure and safe as much as possible from disasters (natural and man-made) | • Have enough spare parts and materials on standby to access and repair asset.<br>• Have a backup asset placed in a secure location for use while main asset is being repaired. |

| Asset | Issue | Risk Matrix | | | Responsive Actions | Preventive Actions | Contingency Actions |
|---|---|---|---|---|---|---|---|
| | | Likelihood | Impact | Risk | | | |
| | | | | | | | |
| | Damaged product (write off) | | | | 1. Inform project leader of loss of asset.<br>2. Dispose of asset (salvage parts if possible).<br>3. Retrieve/Purchase new asset.<br>4. Document issue and actions taken. | • Discuss and accept potential level of damage asset is allowed to take prior to any modifications/tests/uses.<br>• Attempt to carry out uses of asset which could result only in negligible to no damage unless recommendation above is agreed.<br>• Attempt to carry out repairs wherever feasible for damaged sections of asset as soon as possible prior to use.<br>• Ensure location of storage and work environment is secure and safe as much as possible from disasters (natural and man-made) | • Have spare assets placed in a secure location for immediate use.<br>• Attempt to salvage written-off asset for parts or recuperation of finances if possible. |
| | | | | | | | |
| | Missing product (lost/stolen) | | | | 1.Inform project leader of loss of asset.<br>2.Ensure other assets are secure.<br>3.Inform person in charge of company purchases.<br>4.Retrieve replacement of asset (backup or | • Ensure that the assets are accessible only to authorized members in authorized locations and times (project-specific).<br>• Ensure storage location of asset is secure from unauthorized entry. | • Have a backup asset placed in a secure location for use while main asset is missing.<br>• (if possible) Have templates and spare parts to quickly |

| Asset | Issue | Risk Matrix | | | Responsive Actions | Preventive Actions | Contingency Actions |
|---|---|---|---|---|---|---|---|
| | | Likelihood | Impact | Risk | | | |
| | | | | | purchase).<br>5.Carry out relevant actions to ensure replacement is operational and secure. | | recreate replica of missing asset.<br>• Have enough spare parts and materials on standby to access and repair missing asset if located. |