



**GOOD BOOST**

# **Technology Risk Case Report & Log (#GBP026)**

Reviewed: 16<sup>th</sup> December 2025  
Next review: 16th December 2026  
Reviewed by: Alex Georgiou

## Document Control

|                         |                                                                               |
|-------------------------|-------------------------------------------------------------------------------|
| <b>Organisation</b>     | Good Boost Wellbeing Ltd                                                      |
| <b>Title</b>            | Technology Risk Case Report & Log – GBP026                                    |
| <b>Author</b>           | Alex Georgiou                                                                 |
| <b>Owner</b>            | Alex Georgiou – Chief Technical Officer (CTO) & Data Protection Officer (DPO) |
| <b>Next Review date</b> | 16/12/2026                                                                    |

## Document Approvals

This document requires the following approvals:

| <b>Sponsor Approval</b> | <b>Name</b> | <b>Date</b> |
|-------------------------|-------------|-------------|
| CEO / CSO               | Ben Wilkins | 16/12/2025  |
|                         |             |             |
|                         |             |             |

## Table of Contents

|                                    |           |
|------------------------------------|-----------|
| <b>1. INTRODUCTION AND PURPOSE</b> | <b>4</b>  |
| <b>2. RISK IDENTIFICATION</b>      | <b>4</b>  |
| <b>3. RISK MANAGEMENT STRATEGY</b> | <b>5</b>  |
| <b>4. INCIDENT REPORTING</b>       | <b>7</b>  |
| <b>5. BUSINESS CONTINUITY</b>      | <b>8</b>  |
| <b>6. TERMINATION PROCEDURES</b>   | <b>10</b> |
| <b>7. PHYSICAL SITE SECURITY</b>   | <b>10</b> |
| <b>8. CONCLUSION</b>               | <b>11</b> |

## 1.0 Introduction and Purpose

1.1 Good Boost's technology risk management plan provides the process that identifies information technology associated risk on an ongoing basis, documents identified risks and the response to them the organisation expects. A risk is an event or condition that, if it occurs, could have a positive or negative effect on a project's and/or organisations objectives. Risk Management is the process of identifying, assessing, responding to, monitoring, and reporting risks. This Risk Management Plan defines how risks associated with technology will be identified, analysed, and managed. It outlines how risk management activities will be performed, recorded, and monitored throughout the lifecycle of the project and provides templates and practices for recording and prioritising risks.

The Risk Management Plan is created by the Data Protection Officer (DPO) / Technology Director, is informed and updated by the Clinical Safety Officer (CSO) and is monitored by responsible technology and engineering team members. The intended audience of this document is the technology staff and the wider team for full awareness.

Good Boost's Technology Risk Management plan exists to identify risk within our technology infrastructure, architecture and operation and create plans, actions and protocol to mitigate risk. Furthermore, it is used to monitor and control risk in an effective manner.

The key risks include:

- User suitable technology design
- Clean Code (bug minimisation)
- Version Control
- Malware Attacks / Hacking
- Disaster Recovery

## 1.2 Process

The DPO / Technology Director and the CSO will ensure that risks are actively identified, analysed, and managed throughout the life of the IT resources. Risks will be identified as early as possible to minimize their impact. The steps for accomplishing this are outlined in the following sections. The IT manager responsible for a service will serve as the responsible party for addressing risk in their services

## 1.3 Risk Identification

Risk identification involves the technology leadership (DPO/CSO), appropriate stakeholders, and will include an evaluation of the risks related to the Good Boos technology infrastructure, architecture and operation. The identification effort will take place annually. A Risk Register will be generated and updated as needed and will be stored electronically by the DPO.

### 1.3.1 Three elements of Risk

Good Boost's technology and the processes to deploy them for customer use them are a vital part of the ongoing mission of the organisation and its business goals and objectives. The following describes these three elements in more detail:

**Threats** – threats can be both internal to the organisation and external, and come in many different forms. The common element is they work against the confidentiality, integrity, security and availability of technology, or compromise its function. Some possible threats would be the alteration of data or system, or release of protected information, whether intentional or unintentional. Others would be competitors, hackers and other cyber criminals, acts of terrorism, viruses and malware to names a few.

**Vulnerabilities** – Vulnerability are weaknesses or ‘holes’ in information and technology resources and processes which allow the potential for unauthorised or unintentional change or manipulation of resources which impacts the confidentiality, integrity, security and availability of these technology resources.

**Impacts** – Impacts are the costs associations with failure in protecting the confidentiality, integrity, security and availability of technology resources. These costs can be increased expenses or outflows (fines, work house, equipment replacements, legal fees etc) or decreased revenues due to inability to deliver organisational products and services or negative publicity.

The threats, vulnerabilities and impacts to information resources are not constant and will change over time. Because of this, the threats to vulnerability of the overall impact of every technology resources must be evaluated and re-evaluated on a regular basis to ensure the ongoing risks are continuously managed.

## 1.4 Quantitative Estimation of Technology Risk

Estimation of technology risk uses criteria specified below that includes:

- Severity of the hazard
- Likelihood of the hazard
- The resulting clinical risk

To estimate the technology risk a Technical Risk Matrix has been applied to quantify the total risk and the risk acceptability definitions suitably evaluate and respond to each risk.

The Technology Risk Matrix and scoring criteria are displayed below

### Technology Risk Matrix

|                   |           |                 |             |              |       |              |
|-------------------|-----------|-----------------|-------------|--------------|-------|--------------|
| <b>Likelihood</b> | Very High | 3               | 4           | 4            | 5     | 5            |
|                   | High      | 2               | 3           | 3            | 4     | 5            |
|                   | Medium    | 2               | 2           | 3            | 3     | 4            |
|                   | Low       | 1               | 2           | 2            | 3     | 4            |
|                   | Very Low  | 1               | 1           | 2            | 2     | 3            |
|                   |           | Minor           | Significant | Considerable | Major | Catastrophic |
|                   |           | <b>Severity</b> |             |              |       |              |

### Risk Matrix Score Acceptability Definition

| Overall Risk Matrix Score | Risk Definition | Risk Acceptability > Action                                                                                                                                                                                                                |
|---------------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5                         | Very high       | Unacceptable level of risk. Mandatory elimination or control to reduce risk to an acceptable level                                                                                                                                         |
| 4                         | High            | Unacceptable level of risk. Mandatory elimination or control to reduce risk to an acceptable level                                                                                                                                         |
| 3                         | Significant     | Undesirable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternative risks. |
| 2                         | Moderate        | Tolerable where further risk reduction is not practical or impractical without introducing alternative risks.                                                                                                                              |
| 1                         | Low             | Acceptable, no further action required                                                                                                                                                                                                     |

## Likelihood Classification

| Likelihood Category | Interpretation                                                                       |
|---------------------|--------------------------------------------------------------------------------------|
| <b>Very high</b>    | Certain or almost certain; highly likely to occur                                    |
| <b>High</b>         | Not certain but very possible: reasonable expected to occur in the majority of cases |
| <b>Medium</b>       | Possible                                                                             |
| <b>Low</b>          | Could occur but in the great majority of occasions will not                          |
| <b>Very Low</b>     | Negligible or nearly negligible possibility of occurring                             |

## Severity Classification

| Severity Category   | Interpretation                                                                                                                                                                                                                                                                                                  |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Catastrophic</b> | The vulnerability is exposed and exploitable, and it's exploitation could result in severe impacts and of loss of technology system(s) and severe business interruption or failure.                                                                                                                             |
| <b>Major</b>        | The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation could result in considerable exploitation and significant and long-term failure of technology system(s). Relevant controls or remediation is minimally implemented and have limited effectiveness |
| <b>Considerable</b> | The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation could result in moderate exploitation and moderate or temporary failure of technology system(s). Relevant controls or remediation is partially implemented and somewhat effective                 |
| <b>Significant</b>  | The vulnerability is of minor concern, but effectiveness of remediation could be improved                                                                                                                                                                                                                       |
| <b>Minor</b>        | The vulnerability is not of concern. Relevant controls or other remediation is implemented, assessed and effective                                                                                                                                                                                              |

## 2. Risk Identification

In accordance with the technology risk management process a technology risk identification has been undertaken to understand the risks associated with use of Good Boost's digital exercise app and wider technology system. Section 2 described the process and methodology in identifying and analysing risks alongside the estimation of the relative risk to users.

### 2.1 Risk Identification process and Estimation of Technology Risk

Possible risks are explored and identified by the DPO and CSO on an annual basis. This includes reviewing all systems and potential risks to the infrastructure, architecture and operation of Good Boost's technology. The process is a shared activity to list all possible risks and the number of possible contributing causes. The risk rating of likelihood, severity and overall risk is the pre-mitigation risk analysis. Post-mitigation analysis will be complete following application of controls and mitigation actions.

| I.D. | Describe risk and nature of impact                                                                                                                                                                                                                                                               | Likelihood | Severity     | Overall Risk |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|--------------|--------------|
| R1   | Poorly designed and unusable technology for users <ul style="list-style-type: none"> <li>Inability for users to access and utilise Good Boost technology</li> </ul>                                                                                                                              | Medium     | Major        | Medium       |
| R2   | Failure of user facing technology due to overloading <ul style="list-style-type: none"> <li>Inability for users to access and utilise Good Boost technology</li> </ul>                                                                                                                           | Low        | Major        | Medium       |
| R3   | Unauthorised access and use of user personal data <ul style="list-style-type: none"> <li>Data protection compromise; breach of sensitive data</li> </ul>                                                                                                                                         | Medium     | Catastrophic | High         |
| R4   | Errors in data storage and writing to databases <ul style="list-style-type: none"> <li>Inability for users to access and utilise Good Boost technology</li> <li>Potential error in exercise recommendation function</li> </ul>                                                                   | Medium     | Major        | Medium       |
| R5   | Deployment of non-functioning technology due to poor code review <ul style="list-style-type: none"> <li>Inability for users to access and utilise Good Boost technology</li> <li>Incorrect functioning that could lead to data errors of functional errors of exercise recommendation</li> </ul> | Medium     | Major        | Medium       |
| R6   | Malware / Hacking of technology and data <ul style="list-style-type: none"> <li>Loss of company intellectual property</li> <li>Non-functioning of technology</li> <li>Data protection compromise; breach of sensitive data</li> </ul>                                                            | Medium     | Catastrophic | High         |
| R7   | Loss of data due to employee actions <ul style="list-style-type: none"> <li>Loss of company intellectual property</li> <li>Data protection compromise; breach</li> </ul>                                                                                                                         | Medium     | Catastrophic | High         |

|            |                                                                                                                                                                                                                                            |        |              |      |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|--------------|------|
|            | of sensitive data                                                                                                                                                                                                                          |        |              |      |
| <b>R8</b>  | Loss of data due to 3 <sup>rd</sup> parties and contractors <ul style="list-style-type: none"> <li>Loss of company intellectual property</li> <li>Data protection compromise; breach of sensitive data</li> </ul>                          | Medium | Catastrophic | High |
| <b>R9</b>  | Failure of database and cloud storage systems <ul style="list-style-type: none"> <li>Loss of company intellectual property</li> <li>Non-functioning of technology</li> <li>Data protection compromise; breach of sensitive data</li> </ul> | Medium | Catastrophic | High |
| <b>R10</b> | Failure of Clinical Technology systems (such as exercise recommendation errors) <ul style="list-style-type: none"> <li>Incorrect functioning that could lead to data errors of functional errors of exercise recommendation</li> </ul>     | Medium | Catastrophic | High |

## 2.2 Technology Risk Evaluation

| I.D.      | Describe risk and nature of impact                   | Overall Risk | Action                                                                                                                                                                                                                                   |
|-----------|------------------------------------------------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>R1</b> | Poorly designed and unusable technology for users    | Medium       | Unacceptable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks |
| <b>R2</b> | Failure of user facing technology due to overloading | Medium       | Unacceptable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks |
| <b>R3</b> | Unauthorised access and use of user personal data    | High         | Unacceptable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks |
| <b>R4</b> | Errors in data storage and writing to databases      | Medium       | Unacceptable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks |
| <b>R5</b> | Deployment of non-functioning technology due         | Medium       | Unacceptable level of risk. Attempts should be made to eliminate or control                                                                                                                                                              |

## Technology Risk Case Report & Log

|            |                                                                                 |      |                                                                                                                                                                                                                                          |
|------------|---------------------------------------------------------------------------------|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            | to poor code review                                                             |      | to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks                                                                             |
| <b>R6</b>  | Malware / Hacking of technology and data                                        | High | Unacceptable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks |
| <b>R7</b>  | Loss of data due to employee actions                                            | High | Unacceptable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks |
| <b>R8</b>  | Loss of data due to 3 <sup>rd</sup> parties and contractors                     | High | Unacceptable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks |
| <b>R9</b>  | Failure of database and cloud storage systems                                   | High | Unacceptable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks |
| <b>R10</b> | Failure of Clinical Technology systems (such as exercise recommendation errors) | High | Unacceptable level of risk. Attempts should be made to eliminate or control to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical or impossible without introducing alternate risks |

## 2.3 Single and Multiple Contributors to Risks

| I.D. | Describe risk and nature of impact                                              | Contributors                                                                                                                                                                                         |
|------|---------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| R1   | Poorly designed and unusable technology for users                               | <ul style="list-style-type: none"> <li>No user-led design / co-design</li> <li>No internal testing &amp; review</li> <li>No user-led testing / piloting</li> </ul>                                   |
| R2   | Failure of user facing technology due to overloading                            | <ul style="list-style-type: none"> <li>No load testing</li> <li>Use of systems and servers with limited bandwidth</li> </ul>                                                                         |
| R3   | Unauthorised access and use of user personal data                               | <ul style="list-style-type: none"> <li>Failure of Access controls</li> <li>Cyber attack (hacking)</li> </ul>                                                                                         |
| R4   | Errors in data storage and writing to databases                                 | <ul style="list-style-type: none"> <li>No internal testing &amp; review</li> <li>Poor database architecture</li> </ul>                                                                               |
| R5   | Deployment of non-functioning technology due to poor code review                | <ul style="list-style-type: none"> <li>Poor code framework and protocol</li> <li>Poor code review process</li> <li>No internal testing / piloting</li> <li>No user-led testing / piloting</li> </ul> |
| R6   | Malware / Hacking of technology and data                                        | <ul style="list-style-type: none"> <li>No penetration testing</li> <li>Poor/exposed staff operations (i.e. passwords, equipment, network access, training)</li> </ul>                                |
| R7   | Loss of data due to employee actions                                            | <ul style="list-style-type: none"> <li>Poor/exposed staff operations (i.e. passwords, equipment, network access, training)</li> <li>Failure of Access controls</li> </ul>                            |
| R8   | Loss of data due to 3 <sup>rd</sup> parties and contractors                     | <ul style="list-style-type: none"> <li>Poor procurement process</li> <li>Failure of Access controls</li> </ul>                                                                                       |
| R9   | Failure of database and cloud storage systems                                   | <ul style="list-style-type: none"> <li>Poor procurement process</li> <li>Poor database architecture</li> <li>No penetration testing</li> </ul>                                                       |
| R10  | Failure of Clinical Technology systems (such as exercise recommendation errors) | <ul style="list-style-type: none"> <li>Failure of Clinical Risk Management</li> </ul>                                                                                                                |

### 3. Risk Mitigation and Control Planning

Each major risk (those falling in Medium (orange), High (bronze) and Very High (Red) zones on the Risk Matrix) will be assigned to a responsible IT Manager for monitoring purposes to mitigate and reduce risk to a tolerable level. For each major risk, and the single or multiple contributing factors, one of the following approaches will be selected to address it:

- Avoid – eliminate the threat by eliminating the cause
- Mitigate – Identify ways to reduce the probability or the impact of the risk
- Accept – Nothing will be done
- Transfer – Make another party responsible for the risk (buy insurance, outsourcing, etc.)

For each major risk (medium or higher) that will be mitigated, the ultimate accountability is with the Technical Director / DPO to identify ways to prevent the risk from occurring or reduce its impact or probability of occurring. This may include redesign, redevelopment, additional access controls, non-technical administrative controls, new or changed processes, etc.

For each major risk (medium or higher) that is to be mitigated or that is accepted, a course of action will be outlined for the event that the risk does materialise in order to minimise its impact.

### 4. Risk Mitigation Actions

| I.D.      | Describe risk and nature of impact (Rx)                                                                                                                                                                                                                                                                                                                                 | Contributors (Cx) |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| <b>R1</b> | <b>Poorly designed and unusable technology for users</b>                                                                                                                                                                                                                                                                                                                |                   |
| <b>C1</b> | <b>No user-led design / co-design</b><br><b>Action</b> – focus groups with key stakeholder and anticipated users of the technology to co-design the functionality of the technology and ensure technology is inclusive and accessible. Outcomes of focus groups are to be integrated into the iterative design, development and deployment of technology.               |                   |
| <b>C2</b> | <b>No internal testing &amp; review</b><br><b>Action</b> – New releases of the Good Boost app is reviewed by an appointed quality assessor (QA) to systematically check for functioning of technology. Any failures are reported to appropriate teams (technology/clinical) to resolve the failure.                                                                     |                   |
| <b>C3</b> | <b>No user-led testing / piloting</b><br><b>Action</b> – New apps and features are tested by primary user groups (i.e. adults with MSK condition) with feedback loops on functionality and satisfaction. Feedback is reported to relevant teams (technical/clinical) for iterative improvements ahead of final sign off and release of any app, new version or feature. |                   |
| <b>R2</b> | <b>Failure of user facing technology due to overloading</b>                                                                                                                                                                                                                                                                                                             |                   |
| <b>C1</b> | <b>No load testing</b><br><b>Action</b> – Monthly load testing the app and systems that have public facing users to a minimum of double estimated maximum usage (users/end-point calls)                                                                                                                                                                                 |                   |
| <b>C2</b> | <b>Use of systems and servers with limited bandwidth</b><br><b>Action</b> – Procurement of code bases and servers with bandwidth that is sufficient to offer a minimum of double the estimated maximum usage (users/end-point calls)                                                                                                                                    |                   |

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>R3<br/>C1</b> | <b>Unauthorised access and use of user personal data</b><br><b>Failure of Access controls</b><br><b>Action</b> – Access control policy and protocol to minimise staff access to personal data. Two-factor authentication for personal data access. Additional agreements and justification with authorised personnel to have access to this data.                                                                                                |
| <b>C2</b>        | <b>Cyber attack (hacking)</b><br><b>Action</b> – Monthly penetration testing to identify system exposure. Any weaknesses are identified and resolved<br><b>Action</b> – Policies and protocols on employee equipment security, passwords, network access, confidentiality agreements to minimise risk of system access compromise                                                                                                                |
| <b>R4<br/>C1</b> | <b>Errors in data storage and writing to databases</b><br><b>No internal testing &amp; review</b><br><b>Action</b> – New releases of the Good Boost app is reviewed by an appointed quality assessor (QA) to systematically check for functioning of technology. Any failures are reported to appropriate teams (technology/clinical) to resolve the failure.                                                                                    |
| <b>C2</b>        | <b>Poor database architecture</b><br><b>Action</b> – Databases designed to be easy to navigate with data dictionaries to define and explain data stored in databases.<br><b>Action</b> – Routine data accuracy testing to ensure that data entered through front-end apps are accurately recorded in the database                                                                                                                                |
| <b>R5<br/>C1</b> | <b>Deployment of non-functioning technology due to poor code review</b><br><b>Poor code framework and protocol</b><br><b>Action</b> – Follow guidance and framework for clean and maintainable code. All code is subject to review and approval by two developers.                                                                                                                                                                               |
| <b>C2</b>        | <b>Poor code review process</b><br><b>Action</b> - All code is subject to review and approval by two developers and unit testing                                                                                                                                                                                                                                                                                                                 |
| <b>C3</b>        | <b>No internal testing / piloting</b><br><b>Action</b> – New releases of the Good Boost app is reviewed by an appointed quality assessor (QA) to systematically check for functioning of technology. Any failures are reported to appropriate teams (technology/clinical) to resolve the failure.                                                                                                                                                |
| <b>C4</b>        | <b>No user-led testing / piloting</b><br><b>Action</b> – New apps and features are tested by primary user groups (i.e. adults with MSK condition) with feedback loops on functionality and satisfaction. Feedback is reported to relevant teams (technical/clinical) for iterative improvements ahead of final sign off and release of any app, new version or feature                                                                           |
| <b>R6<br/>C1</b> | <b>Malware / Hacking of technology and data</b><br><b>No penetration testing</b><br><b>Action</b> – Quarterly penetration testing. Any exposures and weaknesses are identified and resolved within 5 business days.                                                                                                                                                                                                                              |
| <b>C2</b>        | <b>Poor/exposed staff operations (i.e. passwords, equipment, network access, training)</b><br><b>Action</b> – Implementation of policies and protocol of provision of secure digital equipment and devices, working from home policies, password policies, data protection policies and training to minimise everyday activities of personnel that could compromise exposer and create weaknesses                                                |
| <b>R7<br/>C1</b> | <b>Loss of data due to employee actions</b><br><b>Poor/exposed staff operations (i.e. passwords, equipment, network access, training)</b><br><b>Action</b> – Implementation of policies and protocol of provision of secure digital equipment and devices, working from home policies, password policies, data protection policies and training to minimise everyday activities of personnel that could compromise exposer and create weaknesses |
| <b>C2</b>        | <b>Failure of Access controls</b><br><b>Action</b> – Access control policy and protocol to minimise staff access to personal data. Two-factor authentication for personal data access. Additional agreements and justification with authorised personnel to have access to this data.                                                                                                                                                            |

|            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>R8</b>  | <b>Loss of data due to 3<sup>rd</sup> parties and contractors</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>C1</b>  | <b>Poor procurement process</b><br><b>Action</b> – all 3 <sup>rd</sup> parties must have evidence of acceptable security standards that comply with relevant regulatory standards and practices in place before procurement. All contracts include confidentiality, data sharing agreements and IP/source code ownership<br><b>Action</b> – all sub-contractors agree contracts with clauses of confidentiality and IP ownership. Sub-contractors are provided with Good Boost emails so all communication is centralised and controlled |
| <b>C2</b>  | <b>Failure of Access controls</b><br><b>Action</b> – Access control policy and protocol to minimise staff access to personal data. Two-factor authentication for personal data access. Additional agreements and justification with authorised personnel to have access to this data. Any access of data provided to 3 <sup>rd</sup> parties must follow GDPR requirements and have a minimum sign off of two authorised persons.                                                                                                        |
| <b>R9</b>  | <b>Failure of database and cloud storage systems</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>C1</b>  | <b>Poor procurement process</b><br><b>Action</b> – All digital system must be purchased from a reputable source/organisation<br><b>Action</b> – All digital systems must demonstrate evidence of acceptable standards that comply with relevant regulatory standards and practices.                                                                                                                                                                                                                                                      |
| <b>C2</b>  | <b>Poor database architecture</b><br><b>Action</b> – Databases designed to be easy to navigate with data dictionaries to define and explain data stored in databases.<br><b>Action</b> – Routine data accuracy testing to ensure that data entered through front-end apps are accurately recorded in the database                                                                                                                                                                                                                        |
| <b>C3</b>  | <b>No penetration testing</b><br><b>Action</b> – Quarterly penetration testing. Any exposures and weaknesses are identified and resolved within 5 business days.                                                                                                                                                                                                                                                                                                                                                                         |
| <b>R10</b> | <b>Failure of Clinical Technology systems (such as exercise recommendation errors)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>C1</b>  | <b>Failure of Clinical Risk Management</b><br><b>Action</b> – complete and implement Clinical Risk Management plan                                                                                                                                                                                                                                                                                                                                                                                                                       |

|            |           |          |             |              |       |              |
|------------|-----------|----------|-------------|--------------|-------|--------------|
| Likelihood | Very High | 3        | 4           | 4            | 5     | 5            |
|            | High      | 2        | 3           | 3            | 4     | 5            |
|            | Medium    | 2        | 2           | 3            | 3     | 4            |
|            | Low       | 1        | 2           | 2            | 3     | 4            |
|            | Very Low  | 1        | 1           | 2            | 2     | 3            |
|            |           | Minor    | Significant | Considerable | Major | Catastrophic |
|            |           | Severity |             |              |       |              |

## 4.1 Post-Mitigation Risk Analysis

| I.D. | Describe risk and nature of impact                                              | Likelihood | Severity     | Overall Risk | Mitigation Actions                                                                                                                    | Likelihood | Severity     | Overall Risk |
|------|---------------------------------------------------------------------------------|------------|--------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------|------------|--------------|--------------|
| R1   | Poorly designed and unusable technology for users                               | Medium     | Major        | High         | C1 User-led design / co-design<br>C2 Internal testing & review<br>C3 User-led testing / piloting                                      | Very Low   | Considerable | Moderate     |
| R2   | Failure of user facing technology due to overloading                            | Low        | Major        | High         | C1 Load testing<br>C2 Use of systems and servers with suitable bandwidth                                                              | Low        | Significant  | Moderate     |
| R3   | Unauthorised access and use of user personal data                               | Medium     | Catastrophic | High         | C1 Access controls<br>C2 Cyber attack (hacking) mitigation                                                                            | Very Low   | Major        | Moderate     |
| R4   | Errors in data storage and writing to databases                                 | Medium     | Major        | High         | C1 Internal testing & review<br>C2 Suitable database architecture                                                                     | Very Low   | Significant  | Low          |
| R5   | Deployment of non-functioning technology due to poor code review                | Medium     | Major        | Significant  | C1 Suitable code framework and<br>C2 Suitable code review process<br>C3 Internal testing / piloting<br>C4 User-led testing / piloting | Very Low   | Significant  | Low          |
| R6   | Malware / Hacking of technology and data                                        | Medium     | Catastrophic | High         | C1 Penetration testing<br>C2 Suitable staff operations (i.e. passwords, equipment, network access, training)                          | Very Low   | Major        | Moderate     |
| R7   | Loss of data due to employee actions                                            | Medium     | Catastrophic | High         | C1 Suitable staff operations (i.e. passwords, equipment, network access, training)<br>C2 Access controls                              | Low        | Considerable | Moderate     |
| R8   | Loss of data due to 3 <sup>rd</sup> parties and contractors                     | Medium     | Catastrophic | High         | C1 Suitable procurement process<br>C2 Access Controls                                                                                 | Low        | Considerable | Moderate     |
| R9   | Failure of database and cloud storage systems                                   | Medium     | Catastrophic | High         | C1 Suitable procurement process<br>C2 Access Controls<br>C3 Penetration Testing                                                       | Very Low   | Major        | Moderate     |
| R10  | Failure of Clinical Technology systems (such as exercise recommendation errors) | Medium     | Catastrophic | High         | C1 Suitable Clinical Risk Management                                                                                                  | Very Low   | Major        | Moderate     |

## 4.2 Implementation of Technology Mitigation and Control Measures

The technology risk mitigation actions identified in section 4 must be implemented except where these are to be implemented by another. Every technology risk control measure implemented must be verified and documented by a senior member of each team (technical, clinical, operations).

Every technology risk control measure implemented must have the effectiveness of each measure verified.

## 4.2 Post-Mitigation & Control Technology Risk Evaluation

| I.D. | Describe risk and nature of impact                                              | Overall Risk | Action                                                                                                        |
|------|---------------------------------------------------------------------------------|--------------|---------------------------------------------------------------------------------------------------------------|
| R1   | Poorly designed and unusable technology for users                               | Moderate     | Tolerable where further risk reduction is not practical or impractical without introducing alternative risks. |
| R2   | Failure of user facing technology due to overloading                            | Moderate     | Tolerable where further risk reduction is not practical or impractical without introducing alternative risks. |
| R3   | Unauthorised access and use of user personal data                               | Moderate     | Tolerable where further risk reduction is not practical or impractical without introducing alternative risks. |
| R4   | Errors in data storage and writing to databases                                 | Low          | Acceptable, no further action required                                                                        |
| R5   | Deployment of non-functioning technology due to poor code review                | Low          | Acceptable, no further action required                                                                        |
| R6   | Malware / Hacking of technology and data                                        | Moderate     | Tolerable where further risk reduction is not practical or impractical without introducing alternative risks. |
| R7   | Loss of data due to employee actions                                            | Moderate     | Tolerable where further risk reduction is not practical or impractical without introducing alternative risks. |
| R8   | Loss of data due to 3 <sup>rd</sup> parties and contractors                     | Moderate     | Tolerable where further risk reduction is not practical or impractical without introducing alternative risks. |
| R9   | Failure of database and cloud storage systems                                   | Moderate     | Tolerable where further risk reduction is not practical or impractical without introducing alternative risks. |
| R10  | Failure of Clinical Technology systems (such as exercise recommendation errors) | Moderate     | Tolerable where further risk reduction is not practical or impractical without introducing alternative risks. |

### 4.3 Extended Technology Risk Register

The following risks supplement R1-R10 and are intended to reflect additional technology, cyber-security, cloud and operational risks relevant to Good Boost's current digital service. These risks should be assessed using the same likelihood, severity, overall-risk and post-mitigation methodology already defined in this Technology Risk Management Plan.

| I.D. | Describe risk and nature of impact                                  | Contributors / examples                                                                                    | Suggested controls                                                                                                                  |
|------|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| R11  | Loss or compromise of privileged credentials                        | Compromised AWS, database, source-code, production or administrative credentials.                          | MFA; least privilege; separate privileged accounts; credential rotation; access reviews; rapid revocation.                          |
| R12  | Ransomware or destructive cyber attack                              | Malware, malicious encryption, deletion or corruption affecting systems, code or data.                     | Endpoint protection; immutable/versioned backups where practicable; restore testing; network/access controls; incident response.    |
| R13  | Software supply-chain or dependency compromise                      | Compromised third-party package, library, build dependency or supplier.                                    | Dependency scanning; supplier review; lockfiles/version control; restricted CI/CD permissions; patching process.                    |
| R14  | Critical cloud or external service outage                           | Failure of hosting, DNS, database, authentication, monitoring or other critical external service.          | Resilient architecture; documented dependencies; failover/recovery procedures; supplier monitoring; continuity plan.                |
| R15  | Backup failure or inability to restore                              | Backups incomplete, corrupt, inaccessible or not usable when required.                                     | Automated backup monitoring; separate backup location; periodic restore tests; documented RPO/RTO; evidence of successful restores. |
| R16  | Incorrect infrastructure or production configuration                | Misconfiguration of IAM, firewall/security groups, TLS, DNS, environment variables or production services. | Peer review; infrastructure/change control; least privilege; configuration checks; rollback plan; secrets management.               |
| R17  | Known vulnerabilities in operating systems or software dependencies | Unsupported software, delayed security patches or vulnerable packages expose production systems.           | Vulnerability scanning; patch-management process; severity-based remediation targets; dependency monitoring.                        |
| R18  | Failure of security logging, monitoring or alerting                 | Security incident or system compromise occurs without timely detection.                                    | Centralised logs; alerting; audit trails; log retention; periodic alert testing and review.                                         |
| R19  | Denial of service or malicious traffic                              | High-volume or abusive traffic degrades availability for legitimate users.                                 | Rate limiting; load testing; cloud protection; monitoring; scaling; incident response and recovery procedures.                      |
| R20  | CI/CD, source repository or deployment pipeline compromise          | Unauthorised or malicious code or configuration is introduced into production.                             | MFA; branch protection; code review; restricted deployment rights; secrets protection; audit logging; release approval.             |

## 4.4 Control Assurance, Residual Risk and Evidence

For each risk assessed as Medium or higher, Good Boost should record the effectiveness of the implemented control and the residual risk remaining after controls have been applied. The purpose is to provide an auditable link between the identified risk, the control applied, the person responsible for the control and evidence that the control is operating effectively.

### Minimum control-assurance fields

| Field                            | Requirement                                                                                                              |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Risk / control reference         | Link to the relevant Rx/Cx entry and control action.                                                                     |
| Control owner                    | Named role or individual accountable for operating the control.                                                          |
| Evidence                         | Examples: test report, restore log, access review, deployment record, training record, security scan or incident ticket. |
| Test / review frequency          | How often the control is checked or exercised.                                                                           |
| Last verified date               | Most recent date on which effectiveness was confirmed.                                                                   |
| Residual likelihood and severity | Re-score the risk after controls have been applied.                                                                      |
| Residual risk acceptance         | Record the person approving any residual risk and the basis for acceptance.                                              |
| Next review / target action date | Date for re-testing, treatment or further risk reduction.                                                                |

Where a control cannot be verified or is not operating effectively, the relevant risk must be re-evaluated and a corrective action recorded. Residual High or Very High risks require documented senior approval before continued operation.

## 4.5 Business Continuity and Disaster Recovery Objectives

Business continuity and disaster recovery procedures should define measurable recovery objectives for critical technology services. These values must reflect what Good Boost can actually deliver and should be reviewed following significant architecture changes or recovery tests.

**Required recovery information:** Recovery Time Objective (RTO); Recovery Point Objective (RPO); critical service dependencies; backup location and retention; responsible recovery owner; recovery sequence; and the date/result of the most recent restore or recovery exercise.

Restore testing should confirm not only that backup files exist but that Good Boost can recover a usable service and data set within the documented recovery objectives.

## 4.6 Incident Severity, Vulnerability Management and Triggered Reviews

Technology incidents should be classified so that response times and escalation are proportional to impact. Good Boost may use the following framework and align it with existing incident reporting procedures.

### Incident severity

| Level           | Example                                                                                   | Expected response                                                                      |
|-----------------|-------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| SEV1 - Critical | Major outage, confirmed breach, destructive attack, unsafe clinical technology behaviour. | Immediate escalation to CTO/DPO/CSO; containment and recovery initiated without delay. |
| SEV2 - High     | Material degradation, high-risk vulnerability or suspected compromise.                    | Same-day technical owner assignment and priority remediation.                          |
| SEV3 - Medium   | Limited service issue or vulnerability with compensating controls.                        | Planned remediation with documented target date.                                       |
| SEV4 - Low      | Minor issue with low operational/security impact.                                         | Address through normal maintenance or release process.                                 |

### Vulnerability management

Penetration testing should be supplemented by routine vulnerability and dependency management. Findings should be prioritised by severity and exploitability. Remediation targets should be defined by Good Boost and recorded in the risk or issue log; Critical and High findings should be treated more urgently than Medium or Low findings.

### Security monitoring

Good Boost should maintain appropriate logs and alerts for authentication failures, privileged activity, production changes, deployments, unusual API activity and security events. Log retention and access should be defined and alerting should be periodically tested.

### Triggered review events

An out-of-cycle review of this Technology Risk Management Plan should be initiated following a significant architecture change, introduction of a new processor or critical supplier, major security incident or personal-data breach, material vulnerability, regulatory change, new territory, significant change in the user population, or major change to the exercise recommendation / clinical technology system.

Where a technology incident also involves personal data, the incident must be assessed under Good Boost data-breach procedures and the DPIA should be reviewed where the incident changes the risk to individuals.

*These supplementary sections are intended to be read together with Sections 1-6 of GBP026 and do not replace the existing R1-R10 risk entries or control measures.*

## **5. Risk Monitoring, Controlling & Reporting**

Good Boost must establish, document and maintain a process to collect and review reported risk concerns and safety incidence for the technology system following it's deployment.

Good Boost must assess the impact of any such information on the on-going validity of the technology risk management plan.

Where any such evidence is assessed to compromise and expose the technology system(s), Good Boost must take appropriate corrective action in accordance with the Technology Risk Management Plan and document it in the Technology Risk Case Report.

Good Boost must ensure security and exposure related incidents are reported and resolved in a timely manner of 5-business days. If this is not possible, there must be adequate justification for timescale of resolution.

A record of any security incidents, compromise and exposure, including their resolution, must be maintained by Good Boost in the Technology Risk Case Report Log.

## 6. DPO Sign-off

| Item                                                            | Name/position/date  | Notes                                                                                 |
|-----------------------------------------------------------------|---------------------|---------------------------------------------------------------------------------------|
| Measures approved by:                                           | Alex Georgiou       | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by:                                     | Ben Wilkins         | If accepting any residual high risk, consult the ICO before going ahead               |
| DPO advice provided:                                            | No further comments | DPO should advise on compliance, step 6 measures and whether processing can proceed   |
| Summary of DPO advice:                                          |                     |                                                                                       |
| DPO advice accepted or overruled by:                            | Accepted            | If overruled, you must explain your reasons                                           |
| Comments:                                                       |                     |                                                                                       |
| Consultation responses reviewed by:                             | Ben Wilkins         | If your decision departs from individuals' views, you must explain your reasons       |
| Comments:                                                       |                     |                                                                                       |
| This Technology Risk Management Plan will kept under review by: | Alex Georgiou - DPO | The DPO should also review ongoing compliance with TRMP                               |

Signed:



Alex Georgiou – CTO & DPO  
16<sup>th</sup> Dec 2025