

DATED

[DD/MM/YYYY]

SOFTWARE LICENCE AND SUPPORT AGREEMENT

Between

SARD JV LIMITED

AND

[NAME OF BUYING ORGANISATION]

FOR

SARD MULTISOURCE FEEDBACK (360)

Table of Contents

Clause

1. Agreement Overview	1
2. Goals & Objectives	1
3. Periodic Review	1
4. Service Agreement	2
5. Service Management	3
6. User licences and subscriptions	7
7. Additional user subscriptions	9
8. Service Provision, Maintenance and Availability.....	9
9. System upgrades and developments.....	10
SCHEDULE 1 SUBSCRIPTION FEES	11
1. Subscription Fees	11
2. Additional User Subscription Fees.....	11
SCHEDULE 2 SUBSCRIPTION TERM.....	12
SCHEDULE 3 THE SERVICES	13

THIS AGREEMENT is dated [DD/MM/YYYY]

Parties

- (1) **SARD JV LTD.** a company incorporated and registered in England and Wales with company number 07916735 whose registered office is at Unit 76, Innovation Centre, University Road, Canterbury, Kent, CT2 7FG (“**Contractor**”); and
- (2) [**Name of Organisation**] a [Organisation type], registered in [Country], with company number: [XXXXXX] with offices at [XXXXXX].

1. Agreement Overview

This Agreement represents a Service Level Agreement (“SLA” or “Agreement”) between SARD JV and [**Organisation Name**] for the provisioning of IT services required to support and sustain **processes**, utilising SARD **Multisource Feedback (360)**.

This Agreement remains valid until superseded by a revised agreement mutually endorsed by the stakeholders.

This Agreement outlines the parameters of all IT services covered within the service scope as they are mutually understood by the primary stakeholders.

2. Goals & Objectives

The **purpose** of this Agreement is to ensure that the proper elements and commitments are in place to provide consistent IT service support and delivery to the Customer by the Service Provider.

The **goal** of this Agreement is to obtain mutual agreement for IT service provision between the Service Provider(s) and Customer(s).

The **objectives** of this Agreement are to:

- Provide clear reference to service ownership, accountability, roles and/or responsibilities.
- Present a clear, concise and measurable description of service provision to the customer.
- Match perceptions of expected service provision with actual service support & delivery.

3. Periodic Review

This Agreement is valid from the [TBA] outlined herein and is valid until further notice. This Agreement should be reviewed at a minimum once per fiscal year; however, in lieu of a review during any period specified, the current Agreement will remain in effect for the term of the contract.

The Business Relationship Manager (“Document Owner”) is responsible for facilitating regular reviews of this document. Contents of this document may be amended as required, provided mutual agreement is obtained from the primary stakeholders and communicated to all affected parties. The Document Owner will incorporate all subsequent revisions and obtain mutual agreements / approvals as required.

Business Relationship Manager: **[Name]** (SARD JV)

Review Period: Annually

Previous Review Date: [Month/Year]

Next Review Date: [Month/Year]

4. Service Agreement

The following detailed service parameters are the responsibility of the Service Provider in the ongoing support of this Agreement.

4.1. Service Scope

The following Services are covered by this Agreement;

- System supply;
 - **SARD Multisource Feedback (360)**
- Also incorporating the following support elements
 - Customer and system support
 - Monthly system health check

4.2. Customer Requirements

Customer responsibilities and/or requirements in support of this Agreement include:

- Payment for all support costs at the agreed interval.
- Reasonable availability of customer representative(s) when resolving a service related incident or request.

4.3. Service Provider Requirements

Service Provider responsibilities and/or requirements in support of this Agreement include:

- Meeting response times associated with service related incidents.
- Appropriate notification to Customer for all scheduled maintenance.

4.4. Service Assumptions

Assumptions related to in-scope services and/or components include:

- Changes to services will be communicated and documented to all stakeholders.

5. SERVICE MANAGEMENT

Effective support of in-scope services is a result of maintaining consistent service levels. The following sections provide an overview to relevant details on service and support availability, monitoring of in-scope services and related components (for more details see schedule 3).

The Services

5.1. Service / Support Availability

Coverage parameters specific to the service(s) covered in this Agreement are as follows:

- Online and Telephone support: 9:00 A.M. to 5:00 P.M. Monday – Friday
 - Issues and Feedback received outside of office hours will be logged on SARD JV's ticketing system or received on our answering service and answered within 24 hours or the nearest working day.
- Email support: Monitored 9:00 A.M. to 5:00 P.M. Monday – Friday
- Emails received outside of office hours will be logged and responded to within 24 hours or the nearest working day.

5.2. Service Requests / Incident Reporting

5.2.1. Clarification of what constitutes an incident

It should be understood that support queries and minor bug reports are a normal and expected event of running a Web based software service and in this regard what may be considered a reportable customer 'incident' within another industry is considered a 'support ticket' for the purposes of SARD. Whilst there are similarities between the support ticketing system and technical incident reporting, they are two distinct processes. Most support tickets should not be reported as incidents unless they relate to a previously unreported technical incident that is of at least moderate/medium severity and urgency.

The purpose of making this distinction is to ensure that 'incidents' that are outside the normal business operation are not lost within the day-to-day support ticketing system.

Incidents in the context of this management system should be considered events that impact the normal running of the business or compromise data security.

Examples of incidents would be:

- Data loss
- Disclosure of protected data
- Loss of web services
- A non-trivial injury to staff
- Theft or criminal actions
- Near misses of high to medium severity.
- External severe incidents – e.g. a known incident from a competitor or related industry that may influence our own risk register.

Examples of non-incidents

- A technical bug or query that relates to a small group of users.
- A minor injury e.g. a paper cut.
- Lost passwords

5.2.2. Incident Reporting Culture

The reporting of incidents and the maintenance of an effective risk register are a high business priority for SARD JV. The organisation strives to adopt a culture where staff and clients are encouraged to report high severity incidents without fear of disciplinary repercussions.

5.2.3. Procedure

Reporting an incident:

Incidents can be logged through our online chat, by email or phone.

- Email: support@sardjv.co.uk (incidents can be reported here 24/7 but this address is only monitored 9am – 5pm Monday to Friday)
- Phone: 020 3529 2066 (9am – 5pm Monday to Friday)

Logging Priority 1 Incidents outside of core hours

In the event of a priority 1 incident outside of core office hours, the following phone numbers are provided to main client contacts and all SARD Staff. They should be contacted in this order:

Kevin Monk (CEO): 07736 066408

Philip Bottle (Managing Director): 07894 128377

Incident Number

All incidents are given an incident number, which will be quoted in an acknowledgement email as soon as the incident is logged. If you need to correspond further about an incident please include the incident number in the email subject line. The incident number refers to the incident number within the incident log.

If reported via the support ticketing or Live Chat systems, incidents may include an additional support ticket number that should not be confused with the incident reference number.

5.2.4 Legality, Severity, Urgency and Likelihood Definitions

The following severity, urgency and likelihood definitions are used to determine the priority given to an incident and measuring any associated risks:

5.2.4.1 Severity Definitions

Severity definitions for an incident relate to the severity definitions within our Risk Register.

- **High** - An event that, if it occurred, would cause program failure. Complete mission failure, death, or loss of system. Loss of confidentiality, availability or

integrity of data would have considerable and/or immediate impact on cash flow, operations, legal or contractual obligations or reputation of any stakeholders.

- **Moderate** - An event that, if it occurred, would cause moderate cost and schedule increases, but important requirements would still be met. Injury, minor occupational illness, or minor system damage. Loss of confidentiality, availability or integrity of data could incur costs and have a moderate effect upon legal or contractual obligations and the reputation of any stakeholders.
- **Low** - A non-key service has failed, or is degraded, affecting a few users. An event that, if it occurred, would cause only a small cost and schedule increase. Requirements would still be achieved. Loss of confidentiality, availability or integrity of data are not involved.

5.2.4.2 Urgency Definitions

- **Very High** - Critical deadlines are at risk, and no workaround is available.
- **High** - No workaround is available, but there is no immediate deadline or a workaround is available, and there is an immediate deadline.
- **Medium** - A workaround is available, and there is no immediate deadline.

5.2.4.3 Likelihood Definitions

- **Low** – Existing controls are strong and no new incidents are expected in the future
- **Moderate** – Existing controls are moderate and provide an adequate level of protection. Further incidents are possible, but not highly likely
- **High** – Existing controls have been found to be low or ineffective. Such incidents have a high risk of reoccurring in the future

5.2.5 Priority Allocation

Incidents are allocated a priority in the following manner:

		Severity		
		High	Moderate	Low
Urgency	Very High	Priority 1	Priority 2	Priority 3
	High	Priority 2	Priority 3	Priority 4
	Medium	Priority 2	Priority 4	Priority 5

5.2.6 Resolution Target by Priority

	Target Resolution Time	Resolution Target
Priority 1	1 day	90%
Priority 2	3 days	90%
Priority 3	5 days	90%
Priority 4	8 days	90%
Priority 5	15 days	90%

The resolution target time applies to core working hours only: Monday – Friday, 09:00-17:00, excluding Bank Holidays and other closure days.

The majority of incidents will be resolved before the times stated above.

5.2.7 Resolution Times

Resolution time commences from when an incident is logged and an incident reference number is allocated. The resolution time applies to core working hours only: Monday – Friday, 09:00-17:00, excluding Bank Holidays and closure days.

Whilst we aim to resolve all incidents on a permanent basis, our immediate priority is to get users back up and running so they can continue their work, with a longer term solution following. For example if there was a fault that stopped a doctor from completing their appraisal then we may make modifications as administrators that would allow them to continue through the process rather than fix the underlying fault. Resolution target times are therefore based on initial solution.

Where the solution is not permanent:

- For incidents relating to a problem with a single user, we will update you, and put your incident “on hold” until we have fully resolved it, and then close the incident. For example, if an appraisal was not functioning correctly, the incident would not be closed until the doctor could complete their appraisal.
- For an incident that effects the entire group we will update the incident as resolved and close the incident once the temporary solution has been put in place. We would then manage the underlying problem internally until its resolution.

5.2.8 Closing an incident

When an incident is judged to be resolved the Contractor will send the Customer a completion email: if the Contractor does not hear from the Customer within 5 working days suggesting the incident is not resolved, the incident will automatically be closed, and the Customer will be sent an email to this effect. At this point, if the Customer feels the incident has not been resolved, the Customer can reply to the email and the incident will be reopened..

5.3 Communicating Incidents

5.3.4 **Unplanned service downtime**

System administrators will be notified by email (and phone where practical) of unplanned service downtime.

5.3.5 **Service degradation or known faults**

Service degradation and known faults can be communicated to all users via site-wide announcements on the SARD system. Administrators will also be contacted by email.

5.3.6 **Other major incidents (e.g. data loss, data disclosure)**

Other major incidents will be communicated to system administrators and

service managers within the trust. Where appropriate, a meeting may be called to discuss the incident or to provide an incident report

5.4 Data Protection and GDPR Compliance

For the purposes of the UK General Data Protection Regulation (“UK GDPR”) and the Data Protection Act 2018:

The Customer shall be the Data Controller and SARD JV Limited shall act as the Data Processor in respect of all Personal Data processed under this Agreement.

SARD JV Limited shall process Personal Data only on documented instructions from the Customer and solely for the purposes of providing the Services under this Agreement, unless required to do so by applicable law.

SARD JV Limited shall ensure that all persons authorised to process Personal Data are subject to appropriate confidentiality obligations.

SARD JV Limited shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

SARD JV Limited shall assist the Customer, where reasonably required, in responding to requests from data subjects exercising their rights under UK GDPR.

SARD JV Limited shall notify the Customer without undue delay upon becoming aware of any Personal Data Breach affecting Personal Data processed under this Agreement.

Upon termination or expiry of this Agreement, SARD JV Limited shall, at the Customer’s option, return or securely delete Personal Data in accordance with the Data Processor Agreement and applicable data retention requirements.

SARD JV Limited shall make available to the Customer all information reasonably necessary to demonstrate compliance with this clause and shall allow for and contribute to audits conducted by or on behalf of the Customer where required by law or regulation.

6. User licences and subscriptions

6.1. SARD JV grants to the customer, **[Organisations Name]**, a non-exclusive, non-transferable right to permit the customer to use the Services and the Documentation during the Subscription Term solely for the customer’s internal business operations.

6.2. In relation to the customer’s user limitations, the customer organisation undertakes that:

6.2.1. the maximum number of Authorised Users that it authorises to access and use the Services and the Documentation should not exceed the number of User Subscriptions it has purchased from SARD JV, unless agreed prior to the extension;

- 6.2.2. it will not allow any User Subscription to be used by more than one individual user unless it has been reassigned in its entirety to another individual user, in which case the prior user shall no longer have any right to access or use the Services and/or Documentation;
 - 6.2.3. user subscriptions can be used concurrently, as long as the number of active users do not exceed the number of purchased licenses. As such should a user leave the organisation, the user subscription can be taken up by another user up to the originally purchased number of users;
 - 6.2.4. each User shall keep a secure password for his use of the Services and Documentation; that such password shall be changed no less frequently than monthly and that each User shall keep his password confidential;
 - 6.2.5. it shall maintain a written, up to date list of current Authorised Users and provide such list to SARD JV within 5 (five) Business Days of a written request at any time or times;
 - 6.2.6. it shall permit SARD JV to audit the Services in order to establish the name of each current User. Such audit may be conducted no more than once per quarter, at SARD JV's expense, and this right shall be exercised with reasonable prior notice, in such a manner as not to substantially interfere with the Authority's normal conduct of business;
 - 6.2.7. if any of the audits referred to in clause 6.2.6 reveal that any individual who is not an 'Authorised' User has been given access to the Software, the customer shall pay to SARD JV an amount equal to such underpayment as calculated in accordance with the prices set out in paragraph 1 of 0 within 10 (ten) Business Days of the date of the relevant audit to ensure the user can remain on the system.
- 6.3. The Customer shall not (and shall ensure that its Authorised Users, employees, agents and sub-contractors shall not) access, store, distribute or transmit any Viruses, or any material during the course of its use of the Services that:
- 6.3.1. is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive;
 - 6.3.2. facilitates illegal activity;
 - 6.3.3. depicts sexually explicit images;
 - 6.3.4. promotes unlawful violence;
 - 6.3.5. is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; or
 - 6.3.6. in a manner that is otherwise illegal or causes damage or injury to any person or property;
- and SARD JV reserves the right, without liability or prejudice to its other rights to the Authority, to disable the Authority's access to any material that breaches the provisions of this clause.
- 6.4. The Customer shall not (and shall ensure that its Authorised Users, employees, agents and sub-contractors shall not):
- 6.4.1. attempt to copy, modify, duplicate, create derivative works from, frame, mirror, republish, download, display, transmit, or distribute all or any portion of the Software and/or Documentation (as applicable) in any form or media or by any means;

- 6.4.2. access all or any part of the Services and Documentation in order to build a product or service which competes with the Services and/or the Documentation;
 - 6.4.3. access all or any part of the Services and Documentation in order to build a product or service which competes with the Services and/or the Documentation;
 - 6.4.4. use the Services and/or Documentation to provide services to third parties;
 - 6.4.5. license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit, or otherwise make the Services and/or Documentation available to any third party except the Authorised Users, or
 - 6.4.6. attempt to obtain, or assist third parties in obtaining, access to the Services and/or Documentation.
- 6.5. The Customer Organisation shall use all reasonable endeavours to prevent any unauthorised access to, or use of, the Services and/or the Documentation and, in the event of any such unauthorised access or use, promptly notify SARD JV.
- 6.6. The rights provided under this clause 6 are granted to the customer organisation only, and shall not be considered granted to any subsidiary or holding company of customer Organisation.

7. Additional user subscriptions

- 7.1. If the Customer organisation wishes to purchase additional User Subscriptions, the customer shall notify the Contractor as soon as possible.
- 7.2. Upon agreement to supply additional user subscriptions the customer will pay the additional invoice within 30 days of receipt to ensure that the extra user licences can be activated.

8. Service Provision, Maintenance and Availability

- 8.1. SARD JV shall, during the Subscription Term, provide the Services and make available the Documentation to the customer organisation on and subject to the terms of this agreement.
- 8.2. SARD JV shall use commercially reasonable endeavours to make the Services available 24 hours a day, seven days a week, except for:
 - 8.2.1. planned maintenance carried out during the maintenance window of 10.00 pm to 2.00 am UK time; and
 - 8.2.2. unscheduled maintenance performed outside Normal Business Hours, provided that the Contractor has used reasonable endeavours to give the Authority at least 6 Normal Business Hours' notice in advance.
- 8.3. SARD JV as part of the Services and at no additional cost to the Authority, shall provide the customer with standard support services as outlined above.
- 8.4. The contractor agrees to meet the following service availability based on a maximum of **[Number]** concurrent Users of 99.9% system up time and therefore 0.01% service downtime.
- 8.5. Service downtime is defined as the time where not one user is able to access the system and can be calculated as follow:

$$\frac{(\text{Service Hours in Month} - \text{Service Downtime in Month}) \times 100}{\text{Service hours in Month}}$$

8.6. Service Downtime excludes

- Planned maintenance
- Scheduled Interruptions,
- Downtime caused by the Clients ICT environment
 - Including Network / Broadband service provider issues

9. System upgrades and developments

- 9.1. System development and upgrades to the purchased software are included in the per annum fee, however upgrades and development to other modules related to the purchased system can be purchased at any time.
- 9.2. All major system upgrades and developments will be communicated to the customer organisation before commencement of deployment with an opt-out option. This does not apply to routine bug fixes and maintenance.

Schedule 1 - Subscription Fees

1. Subscription Fees

The subscription fees are as outlined in the tender submission / Detailed proposal and as outlined in the full contract offer for **[System Name]** and amounts to **[£X per annum]**

2. Additional User Subscription Fees

Additional User Subscriptions may be purchased at the same rate outlined within the tender submission / Detailed proposal and as outlined in the full contract offer.

Subscription Term

1. Initial Subscription Term: **[X]** Years with the option of a further 12 months.

The Services

1) The Services

A) Service Commissioning

Service	Timescale
Configure a system for access by the Authority and create an account for the Administrator	Within 1 Business Day of receipt of the Advance
Provide an initial training and orientation session in the configuration and administrative functions, and normal operation as a User to the Administrator and selected key members of staff	Within 10 Business Days of receipt of the Advance, assuming availability and co-operation of the Administrator
Provide technical support to the Administrator in creating accounts for the Users of the Authority and in making data configuration choices	Within 10 Business Days of the training and orientation session
Co-operate with the Administrator in confirming the conditions required for Acceptance	Within 15 Business Days of training and orientation session

B) Acceptance Criteria

Administrator is able to:

- i) access the Software;
- ii) add a User;
- iii) upload a document;
- iv) import ESR data;
- v) create medical roles and assign Users;
- vi) create appraisal datasets;
- vii) assign appraisal datasets to medical roles;
- viii) assign directorates for Users;
- ix) assign lead appraisers for Users.

The Contractor

Signed by [NAME OF
AUTHORISED SIGNATORY]

for and on behalf of SARD JV

[Email]

.....

Director

The Authority

Signed by [NAME OF
AUTHORISED SIGNATORY]

for and on behalf of [AUTHORITY]

[Email]

.....

Authorised Signatory