EVALUATION AGREEMENT · REF SSUAE-EVAL-YYYY-###

Enterprise Software Evaluation Agreement

and Service Level Agreement

Terms for evaluating the Site Safety UAE HSE Operations Dashboard on an Enterprise workspace, including availability, support and data protection commitments.

PREPARED FOR	[Customer legal name] [legal form and jurisdiction] Registered address: [full registered address] Notice email: [name@company.com]
PROVIDED BY	Site Safety LLC (trading as Site Safety UAE) Dubai, United Arab Emirates info@sitesafetyuae.com
EVALUATION PERIOD	[30] days from [DD Month YYYY] to [DD Month YYYY]
LICENCE BASIS	Enterprise — [number] project sites, [number] named users
SUPPORT TIER	Enterprise — named account contact, 24–48 hour first response
AVAILABILITY	99.5% monthly Uptime target (Schedule B)
FEES DURING EVALUATION	[Nil / USD ### per month]
GOVERNING LAW	Laws of the United Arab Emirates
JURISDICTION	Courts of the Emirate of Dubai
SIGNATURE METHOD	[wet ink / electronic signature]

This document is confidential to the Parties. It is a commercial template, not yet reviewed by a lawyer (draft prepared for lawyer review), and not legal advice. The Service is provided on a software-only licence: no hired staff, on-site personnel, consulting hours or physical safety officers are bundled with it, and the Customer remains responsible for its own HSE obligations. Each Party should obtain its own legal advice before signing.

Document control

Item	Detail
Document title	Enterprise Software Evaluation Agreement and Service Level Agreement
Document reference	SSUAE-EVAL-TEMPLATE-001
Version	1.2
Status	Draft prepared for lawyer review
Document owner	Founder, Site Safety LLC
Applies to	Every Enterprise evaluation of the Site Safety UAE HSE Operations Dashboard granted by Site Safety LLC
Governing law	Laws of the United Arab Emirates
Jurisdiction	Courts of the Emirate of Dubai
Review cycle	Annually, and on any material change in law, the Service, or the published support and security position
Next review	2 October 2027
Retention of signed copies	Seven years after expiry, then securely destroyed

Document history

Version	Date	Author	Summary of changes
1.0	2 October 2026	Founder, Site Safety LLC	First issue. Enterprise evaluation terms aligned to the published Terms of Service (v1.4), Support SLA and response-time policy (v1.2), Security & Access disclosure, Privacy Policy (v1.3) and Trust & AI Safety guidance, and to the UAE Civil Transactions Law (Federal Decree-Law No. 25 of 2025).

Related agreements and published documents

This Agreement sits inside a framework of published documents. Clause 2 sets out how they interact and which prevails if there is a conflict.

Document	Reference	Role in the framework
Mutual Non-Disclosure Agreement	SSUAE-NDA-TEMPLATE-001	Protects confidential information exchanged during the evaluation. Incorporated by reference under clause 14.
Terms of Service	v1.5, 11 October	Baseline terms for use of the Service. Incorporated

	2026	where this Agreement does not expressly vary them.
Data Processing Agreement	Signed before onboarding	Governs the processing of Personal Data in the Evaluation Workspace. Takes precedence over clause 11 on data protection matters.
Support SLA and response-time policy	v1.2, effective 11 October 2026	Published response targets by plan. Schedule B and Schedule C record the contractual position for this evaluation.
Security & Access disclosure	Current version	Describes the controls in place and the controls not in place. Basis of Schedule D.
Privacy Policy	v1.3, 27 July 2026	How Site Safety UAE handles personal information as controller.
Trust & AI Safety guidance	Current version	How AI features are used, verified and limited. Basis of clause 12.
Refund Policy	Current version	Refund mechanics for any paid subscription that follows the evaluation.

Agreement particulars

The particulars below record the commercial terms of this evaluation. Where a particular is completed in an Order Form signed by both Parties, the Order Form prevails over this table.

Particular	Entry
Evaluation reference	[SSUAE-EVAL-YYYY-###]
Effective date	[DD Month YYYY]
Evaluation period	[30] days from the Effective Date, ending [DD Month YYYY] (clause 5.1)
Customer legal name	[full legal name of the Customer]
Customer legal form and jurisdiction	[e.g. limited liability company, Emirate of Dubai, UAE]
Customer registered address	[full registered address]
Customer notice email	[name@company.com]
Provider notice email	info@sitesafetyuae.com
Customer administrator	[name, job title and email address]
Evaluation Workspace	[workspace name and identifier]
Evaluation environment	[Production workspace / dedicated sandbox workspace]
Licensed modules	[All modules / modules listed in Schedule A]
Active project sites	[number] project sites
Named users	[number] named users
AI assist allowance	[number] AI actions per calendar month, shared across all AI tools
Included storage	[50 GB / 1 TB / other]
Support tier	Enterprise — named account contact and priority escalation
Availability target	99.5% monthly Uptime target (Schedule B)
Data region	[primary region, confirmed in writing under clause 11.9]
Fees during the evaluation period	[Nil / USD ### per month]
Conversion option	Enterprise subscription per the Order Form (clause 5.3)
Service credit remedy	Evaluation-period extension, or subscription credit on conversion (Schedule B)
Signature method	[wet ink / electronic signature]

Contents

Clause	Section	Page
1	Definitions and interpretation	6
2	Structure of this Agreement	8
3	Grant of evaluation licence	8
4	Access, provisioning and user administration	9
5	Evaluation period, extension and conversion	11
6	Fees, payment and taxes	11
7	Service availability target	12
8	Support and escalation	13
9	Disaster recovery, backup and continuity	13
10	Security and assurance	14
11	Data protection	15
12	AI-assisted features	16
13	Customer Content and intellectual property	17
14	Confidentiality	18
15	Service changes and roadmap	18
16	Suspension	19
17	Term and termination	19
18	Consequences of termination	20
19	Warranties and disclaimers	20
20	Limitation of liability	21
21	Indemnities	22
22	Compliance	22
23	Force majeure	23
24	Notices	23
25	Governing law and dispute resolution	23
26	General provisions	24
	Execution	25
Schedule A	Evaluation scope and licensed modules	26
Schedule B	Service Level Agreement	28
Schedule C	Support, severity and escalation	31
Schedule D	Security controls and shared responsibility	33
Schedule E	Service credit claim	35
Schedule F	Authorised users and notice details	35

1. Definitions and interpretation

1.1 Definitions. In this Agreement the following terms have the meanings set out below. A term defined in the singular includes the plural and vice versa.

Term	Meaning
Agreement	This Enterprise Software Evaluation Agreement and Service Level Agreement, including its schedules, as varied under clause 26.2.
AI Action	One invocation of an AI-Assisted Feature that consumes one unit of the Customer's shared monthly AI allowance.
AI-Assisted Feature	Any feature of the Service that uses a machine learning model to draft, summarise, classify, suggest or review content, including MSRA drafting, root-cause suggestion, document review and incident-photo hazard classification.
Availability	The proportion of time in a calendar month during which the core Service is available for use by the Customer, measured in accordance with Schedule B.
Business Day	A day other than a Friday, Saturday or public holiday in the United Arab Emirates.
Confidential Information	Has the meaning given in the Mutual Non-Disclosure Agreement between the Parties, or, if none is in force, the meaning given in clause 14.2.
Customer	The entity identified as the Customer on the cover page and in the Agreement particulars.
Customer Content	All data, documents, images, records, comments and other content uploaded to or created within the Evaluation Workspace by the Customer or its Users, including permits, inspections, incident records, worker records and training records.
Data Processing Agreement / DPA	The data processing agreement between the Parties governing the processing of Personal Data, signed before onboarding.
Downtime	Any period during which the core Service is not available, other than Excluded Downtime, as measured in Schedule B.
Enterprise Plan	The Enterprise subscription described on the Provider's published pricing page at the Effective Date.
Evaluation Period	The period stated in the Agreement particulars during which the Customer may evaluate the Service under this Agreement.
Evaluation Workspace	The logically separated workspace provisioned for the Customer for the purposes of the evaluation.
Excluded Downtime	The periods excluded from the Availability calculation, as listed in Schedule B.
Incident	A single, unplanned event or condition that causes or may cause Downtime or a material degradation of the Service, or a security event

	affecting Customer Content.
Order Form	A written order, quote acceptance or subscription form signed or accepted by both Parties that records the commercial terms of the evaluation or of a subscription following it.
Personal Data	Any information relating to an identified or identifiable natural person, as defined in applicable data protection law, including the UAE Personal Data Protection Law (Federal Decree-Law No. 45 of 2021).
Platform / Service	The Site Safety UAE HSE Operations Dashboard and any related software, applications, interfaces, templates, content and AI-Assisted Features made available by the Provider.
Provider	Site Safety LLC, a limited liability company incorporated in the United Arab Emirates, trading as Site Safety UAE.
Scheduled Maintenance Window	A pre-notified window during which the Provider may perform maintenance, as set out in Schedule B.
Service Credit	The remedy calculated under Schedule B for a failure to meet the Availability target.
Severity Level	The classification of a support ticket as S1, S2 or S3 under Schedule C.
SLA	The service level agreement set out in Schedule B and Schedule C.
Subprocessor	A third party engaged by the Provider to process Customer Content or Personal Data on the Provider's behalf.
Support Hours	The hours during which the Provider provides support, as set out in Schedule C.
Third-Party AI Provider	A third-party provider of machine learning models used to deliver the AI-Assisted Features.
Uptime Percentage	The Availability figure expressed as a percentage and calculated in accordance with Schedule B.
User	An individual named in Schedule F and authorised by the Customer to access the Evaluation Workspace.

1.2 Interpretation. In this Agreement, unless the context requires otherwise: (a) headings are for convenience only and do not affect interpretation; (b) “including”, “includes” and “include” are not limiting; (c) a reference to a statute or regulation includes any amendment, re-enactment or replacement of it; (d) a reference to a clause or schedule is a reference to a clause of, or a schedule to, this Agreement; (e) “writing” includes email and other electronic communication; (f) a reference to a person includes a natural person, body corporate, partnership, joint venture, government body or unincorporated association; (g) “GST” means Gulf Standard Time (UTC+4); and (h) a reference to a month means a calendar month.

1.3 Language. This Agreement is made in the English language. Any translation is provided for convenience only, and the English text prevails in the event of any inconsistency.

2. Structure of this Agreement

2.1 Framework. This Agreement, the Order Form, the DPA and the Terms of Service together govern the evaluation. The Customer's use of the Service is also subject to the Provider's published acceptable use and security policies.

2.2 Incorporation of the Terms of Service. The Provider's Terms of Service (version 1.5, 11 October 2026, or the version in force at the Effective Date) are incorporated into this Agreement, except where this Agreement expressly provides otherwise. Where this Agreement sets a specific service level, support commitment or remedy, that provision applies in place of the general position in the Terms of Service.

2.3 Order of precedence. If there is a conflict between the documents in the framework, the following order of precedence applies, from highest to lowest.

Rank	Document	Scope of precedence
1	A signed Order Form	Prevails over all other documents, but only in respect of the commercial particulars it records.
2	This Agreement and its schedules	Prevails over the Terms of Service, the Privacy Policy and the published support policy on all matters it addresses.
3	The Data Processing Agreement	Prevails over this Agreement on the processing of Personal Data.
4	The Mutual Non-Disclosure Agreement	Prevails over this Agreement on the protection of Confidential Information.
5	The Terms of Service	Applies to all matters not addressed by the documents above.

2.4 Software-only licence. The Service is a software-as-a-service platform. This Agreement grants access to software, tools, templates and hosted features only. It does not include the provision of hired staff, on-site personnel, consulting hours, classroom training or physical safety officers. The Provider does not act as a competent person, authorised signatory or employer on the Customer's behalf, and any guidance given by email does not create a consulting, agency or employment relationship.

2.5 Shared responsibility. The Provider supplies the platform, its controls and the service levels in Schedule B and Schedule C. The Customer remains responsible for assigning roles correctly, off-boarding leavers, the accuracy and lawfulness of Customer Content, and all HSE decisions, inspections, permit approvals, training and regulatory submissions made using the Service. Schedule D records the allocation of responsibilities in detail.

3. Grant of evaluation licence

3.1 Grant. Subject to this Agreement, the Provider grants the Customer a limited, non-exclusive, non-transferable, non-sub-licensable and revocable right to access and use

the Service during the Evaluation Period, solely for the Evaluation Purpose and within the scope recorded in the Agreement particulars and Schedule A.

3.2 Evaluation Purpose. The Evaluation Purpose is the Customer's internal assessment of whether the Service is suitable for its HSE operations, including configuration, workflow testing, data import, user acceptance testing and internal reporting on the outcome of the evaluation.

3.3 Named users only. Access is granted for the named Users recorded in Schedule F. Credentials must not be shared between individuals, and the Customer must not permit any person who is not a named User to access the Evaluation Workspace.

3.4 Restrictions. The Customer shall not: (a) use the Service for any purpose other than the Evaluation Purpose; (b) use the Service to provide services to a third party, or in a service bureau, bureau, outsourcing or time-sharing arrangement; (c) sell, resell, rent, lease, sub-licence or otherwise make the Service available to any third party; (d) copy, modify, translate, adapt or create derivative works of the Service, except as expressly permitted in writing; (e) reverse engineer, decompile, disassemble or attempt to derive the source code, structure, design, model weights, prompts or training data of the Service; (f) use the Service to develop, train or improve a competing or substitute product or service; (g) conduct penetration testing, vulnerability scanning, load testing or other security testing against the Service except under a separate written authorisation with a defined scope; (h) publish or share benchmark results, comparative performance data or test outcomes without the Provider's prior written consent; or (i) remove, obscure or alter any proprietary notice, watermark or attribution.

3.5 Reservation of rights. All rights not expressly granted in this Agreement are reserved to the Provider and its licensors. No licence, assignment or other right in respect of any intellectual property is granted by implication, estoppel or otherwise.

3.6 No production reliance. The evaluation is not a production service. The Customer shall not rely on the Evaluation Workspace as its only system of record for HSE obligations, and shall not treat AI-Assisted output or draft records produced during the evaluation as an authority approval, a competent-person sign-off or evidence for a regulatory submission without independent verification by a qualified person. Clause 19.4 applies.

3.7 Evaluation feedback. The Customer shall provide reasonable feedback on the Service during and at the end of the Evaluation Period, including on any defects, missing capability or usability issues it identifies.

4. Access, provisioning and user administration

4.1 Provisioning. The Provider shall provision the Evaluation Workspace within three (3) Business Days after the Effective Date, or by any date agreed in the Order Form. The Provider shall provide the Customer's administrator with access details and a short onboarding session by video call or email.

4.2 Company-email enforcement. Workspace access may be restricted to the Customer's company email domain. Invitations and password resets are issued through verified email flows. The Customer is responsible for ensuring that the domain configured for the Evaluation Workspace is one it controls.

4.3 Roles. The Service applies role-based permissions. The standard roles and their intended scope are set out below. Roles are stored separately from user profiles and are enforced on the server.

Role	Intended use	Typical holder
Administrator	Full configuration of the workspace, users, roles, sites, templates and retention settings; access to the audit log.	HSE lead or IT administrator
Manager	Create and approve records, manage documents and reports across assigned sites; no user or billing administration.	Project HSE manager
Supervisor	Create and progress records for assigned sites; raise and close permits, inspections and incidents; no workspace configuration.	Site HSE officer or supervisor
Viewer	Read-only access to records and reports within the assigned scope.	Client, consultant or auditor

4.4 Single sign-on. SAML single sign-on is available on the Enterprise Plan and may be enabled for the Evaluation Workspace on request. Automated SCIM directory provisioning and deprovisioning is not currently offered. User lifecycle is managed by the Customer's workspace administrators, and the Customer shall remove or disable access for any User who leaves its organisation or no longer requires access.

4.5 Individual invite tokens. Where an individual needs to contribute to a site workflow but does not have a company email address, the Provider may issue an invite token. A token creates a separate, single-user limited account with access only to that user's own records and files. Such an account is not a User of the Evaluation Workspace and does not give access to the Customer's or any other organisation's information.

4.6 Customer obligations on access. The Customer shall: (a) provide accurate account information and keep it up to date; (b) keep credentials and any second-factor device secure; (c) be responsible for all activity under its Users' accounts; (d) ensure each User has the competence appropriate to the role assigned; and (e) notify the Provider promptly of any suspected unauthorised access.

4.7 Suspension of individual access. The Provider may suspend an individual account where it reasonably believes the account has been compromised, is being used in breach of clause 3.4, or is required to be suspended by law. The Provider shall notify the Customer's administrator promptly and restore access once the ground for suspension has been resolved.

5. Evaluation period, extension and conversion

5.1 Evaluation Period. The evaluation begins on the Effective Date and continues for the period stated in the Agreement particulars, unless extended or terminated earlier under this Agreement.

5.2 Extension. The Parties may extend the Evaluation Period by written agreement. An extension may also arise automatically under Schedule B where a Service Credit is taken as an extension of the evaluation rather than as a monetary credit.

5.3 Conversion to a subscription. The Customer may convert to an Enterprise subscription at any time during the Evaluation Period by signing an Order Form. On conversion: (a) the subscription term and fees are those recorded in the Order Form; (b) this Agreement continues to apply to the extent it is not superseded by the Order Form; and (c) any Service Credit accrued and not yet applied may be taken as a credit against the first invoice, as recorded in the Order Form.

5.4 No automatic charge. The evaluation does not convert automatically into a paid subscription and does not create any automatic charge. No payment instrument is required to begin an evaluation. Billing begins only if and when the Customer signs an Order Form or completes a subscription through the Provider's checkout.

5.5 Position at the end of the evaluation. If the Customer does not convert or extend, access to the Evaluation Workspace ends at the close of the Evaluation Period and clause 18 applies to Customer Content. Where the Customer holds a separate free or personal account, that account is unaffected, except that any workspace it was invited into is removed.

6. Fees, payment and taxes

6.1 Fees during the evaluation. The fees for the Evaluation Period are those recorded in the Agreement particulars. Where the evaluation is provided at no charge, the Provider still provides the service levels in Schedule B and Schedule C, and Service Credits are taken as an extension of the Evaluation Period under Schedule B.

6.2 Conversion fees. Fees for any subscription following the evaluation are those recorded in the Order Form or published on the Provider's pricing page at the date of the Order Form. Enterprise pricing may be tailored to sites, users and volume.

6.3 Payment processing. Self-serve online subscriptions are sold by Site Safety LLC and paid by card through Stripe as payment processor. Enterprise orders under an Order Form may instead be invoiced by the Provider and paid as stated on the invoice. The published 30-day money-back guarantee applies only to card purchases through online checkout, not to purchase-order or invoiced subscriptions; mandatory legal refund rights are unaffected.

6.4 Taxes. Fees are stated exclusive of applicable taxes. Taxes are calculated at checkout based on the Customer's billing location. Each Party is responsible for its own taxes on its own income.

6.5 Overages. Where the Customer exceeds an allowance recorded in the Agreement particulars, such as the monthly AI Action allowance or included storage, the Provider shall notify the Customer's administrator. Overages are charged only where the Order Form or the Customer's subscription provides for them, at the published overage rate. The Provider shall not charge an overage during a no-charge evaluation unless the Order Form expressly permits it.

6.6 No set-off. Neither Party may set off any amount owed to it against an amount owed by it, except where the amount is undisputed or has been determined by a court or arbitral tribunal.

7. Service availability target

7.1 Availability target. The Provider shall use reasonable efforts to make the core Service available to the Customer at an Uptime Percentage of 99.5% in each calendar month. This is a target, not a guarantee: the Provider does not yet hold a measured availability history that evidences it. Service Credits under Schedule B apply when measured uptime falls below the target during the Evaluation Period, calculated in accordance with Schedule B. The Availability target applies to the hosted Service only and to the core Service as defined in Schedule B.

7.2 Measurement. Availability is measured continuously by automated monitoring against the Provider's public health endpoint, with automated outage alerting. The measurement method, the calculation, the treatment of partial degradation and the exclusions are set out in Schedule B.

7.3 Scheduled maintenance. The Provider may perform scheduled maintenance during the Scheduled Maintenance Windows set out in Schedule B. The Provider shall give the Customer's administrator at least seventy-two (72) hours' notice of a Scheduled Maintenance Window that is expected to cause Downtime, and shall use reasonable efforts to minimise its duration and impact.

7.4 Emergency maintenance. Where urgent maintenance is required to protect the security, integrity or stability of the Service, the Provider may act outside a Scheduled Maintenance Window. It shall give the Customer's administrator as much notice as is reasonably practicable and shall publish a short post-incident summary on request. Emergency maintenance carried out in good faith and reported as required is Excluded Downtime, unless it is recurring and reasonably avoidable.

7.5 Service Credits. If the Uptime Percentage in a calendar month falls below the target in clause 7.1, the Customer is entitled to a Service Credit calculated under Schedule B. During a no-charge evaluation, the Service Credit is taken as an extension of the Evaluation Period at no cost.

7.6 Reporting. The Provider shall provide the Customer with a monthly availability summary on request, within five (5) Business Days of the end of the calendar month, showing the measured Uptime Percentage, any Downtime events with duration and cause, and any Service Credit accrued.

7.7 Sole remedy. Service Credits are the Customer's sole and exclusive financial remedy for a failure to meet the Availability target. This does not limit the Customer's rights for a breach of clause 10, clause 11 or clause 14, or any right that cannot lawfully be limited.

8. Support and escalation

8.1 Support scope. The Provider shall provide support through the Enterprise support tier described in Schedule C. Support covers defect reports and platform outages, account, access and billing issues, product questions and guided setup help, and clarification of the Provider's UAE authority report templates.

8.2 Exclusions from support. Support does not include on-site consulting, external audits, classroom training, the preparation of bespoke documents outside what the Service generates, custom development outside the published roadmap, regulatory representation, or a 24-hour telephone hotline. Support is email-first.

8.3 Severity levels. Incidents and requests are classified by Severity Level as set out in Schedule C. The Customer assigns a proposed Severity Level when raising a ticket, and the Provider may reclassify it after triage, giving reasons. Where the Parties disagree and the matter is material, clause 25.3 applies.

8.4 Response and resolution targets. The Provider shall meet the acknowledgement, response and resolution targets set out in Schedule C. Where a fix requires a software change, the Provider shall confirm its diagnosis within the target period, provide a workaround where one exists, and keep the Customer updated until the fix ships.

8.5 Support Hours. Support is provided during Support Hours as set out in Schedule C. The Provider operates a founder-led support model and responds to S1 incidents outside Support Hours on a best-efforts basis.

8.6 Escalation. Either Party may escalate a ticket through the escalation path in Schedule C. The Provider shall provide a named account contact and priority escalation for the Enterprise tier.

8.7 Cooperation. The Customer shall provide the information reasonably required to investigate and resolve a ticket, including a description of the issue, the affected Users and sites, the time the issue was observed, and any error messages or screenshots. Response targets are suspended while the Provider is waiting for information it has reasonably requested.

9. Disaster recovery, backup and continuity

9.1 Backups. The Provider maintains rolling backups of the managed database, with point-in-time recovery available for the retention window applicable to the Evaluation Workspace. Backups are encrypted at rest by the infrastructure provider and are held separately from the production environment.

9.2 Restore targets. Recovery point and recovery time objectives are agreed for Enterprise agreements and recorded in the Order Form. The Provider does not publish a universal

RTO or RPO that it cannot evidence for every deployment, and the targets agreed for this evaluation are those recorded in the Agreement particulars or the Order Form.

9.3 Restore testing. The Provider tests restore procedures periodically and shall, on reasonable written request not more than once in any twelve-month period, demonstrate a restore of Customer Content into a non-production environment using a representative backup, subject to the Customer's written authorisation.

9.4 Customer-side continuity. The Customer shall maintain its own offline or independent copy of HSE records that it is required by law, by a client or by an authority to retain. The Service is a system of record and evidence tool, not a substitute for the Customer's own statutory record-keeping obligations.

9.5 Continuity during the evaluation. Where a material failure prevents use of the Evaluation Workspace for more than five (5) consecutive Business Days, the Customer may extend the Evaluation Period by the period of the failure, without charge, by written notice.

10. Security and assurance

10.1 Security controls. The Provider maintains the controls set out in Schedule D. Those controls are enabled on every workspace by default. The Provider may improve or replace a control provided that the overall level of protection is not materially reduced.

10.2 Certifications and independent testing. The Provider does not hold ISO 27001 or SOC 2 certification, and has not completed an independent penetration test at the Effective Date. The Provider does not claim otherwise. Automated dependency and platform security scanning runs against every release, and the results of that scanning can be discussed under the Mutual Non-Disclosure Agreement. If independent testing or certification is required, the Parties shall agree the scope, timing and cost in the Order Form or a separate written agreement.

10.3 Vulnerability management. The Provider triages reported vulnerabilities, prioritises remediation by severity and impact, and notifies affected Customers of a confirmed vulnerability that requires Customer action without undue delay.

10.4 Vulnerability reporting. The Customer and its Users may report a suspected vulnerability to info@sitesafetyuae.com. The Provider acknowledges reports within two (2) UAE Business Days, keeps the reporter informed, and does not pursue good-faith researchers who avoid privacy violations, data destruction and service disruption.

10.5 Security pack. On request, the Provider shall provide the Customer with its current subprocessor list, data-flow summary, Data Processing Agreement and written responses to a reasonable security questionnaire, before signature if required.

10.6 Customer security responsibilities. The Customer shall assign roles correctly, restrict access on a need-to-know basis, remove access for leavers, protect its own credentials and second-factor devices, and comply with the acceptable use and security policies referenced in clause 2.1. Schedule D allocates responsibilities in detail.

10.7 Audit. The Provider's assurance model is documentation-based. The Customer may audit compliance with this Agreement by reviewing the security pack, the availability report provided under clause 7.6 and the audit log exported from the Evaluation Workspace. On-site audits and audits of the Provider's infrastructure by the Customer are not offered during an evaluation.

10.8 Security incident notification. The Provider shall notify the Customer's administrator without undue delay after confirming a security incident affecting Customer Content, with the facts known at the time, and shall provide a follow-up summary once its review closes.

11. Data protection

11.1 Data Processing Agreement. The Parties shall sign the Data Processing Agreement before Customer Content containing Personal Data is uploaded to the Evaluation Workspace. The Data Processing Agreement governs the processing of that Personal Data and prevails over this clause 11 to the extent of any conflict.

11.2 Roles. For Personal Data within Customer Content, the Customer is the controller and the Provider is the processor. For account, billing, support and marketing information that the Provider collects directly, the Provider is the controller and the Privacy Policy applies.

11.3 Compliance. Each Party shall comply with applicable data protection law, including the UAE Personal Data Protection Law (Federal Decree-Law No. 45 of 2021), its implementing regulations and any applicable free-zone or emirate-level requirements. The Provider does not claim any certification of compliance.

11.4 Subprocessors. The Provider engages subprocessors for hosting, database, authentication, storage, email delivery, payment processing, error monitoring and optional AI inference. The current list is provided with the security pack. The Provider shall give the Customer reasonable notice of the addition or replacement of a subprocessor that processes Personal Data, and the Customer may object on reasonable data protection grounds. If the Parties cannot resolve an objection, the Customer may terminate the evaluation on written notice without charge.

11.5 International transfers. The Provider's infrastructure providers may process data in the United Arab Emirates, the European Economic Area, the United Kingdom or other regions. Where Personal Data is transferred outside the United Arab Emirates, the Provider relies on its providers' safeguards and shall make available the information reasonably required by the Customer to satisfy its own transfer assessment.

11.6 Retention and deletion. Customer Content is retained for as long as the Evaluation Workspace is active. Workspace owners may delete individual records at any time. On closure of the Evaluation Workspace, live data and storage objects are deleted or anonymised within thirty (30) days, excluding backup copies, which expire on their own retention cycle of up to a further thirty (30) days. A written deletion confirmation is available on request.

11.7 Data subject requests. The Provider shall provide reasonable assistance to the Customer in responding to a request from a data subject relating to Personal Data in Customer Content, including by making available the functionality to access, correct, export or delete records. The Customer shall raise such requests with the Provider through the Customer administrator.

11.8 Personal data breach. The Provider shall notify the Customer without undue delay, and in any event within forty-eight (48) hours, after becoming aware of a personal data breach affecting Personal Data in Customer Content, and shall provide the information reasonably required by the Customer to meet its own notification obligations.

11.9 Data residency. At the date of this template the Service is hosted in Ireland (European Union); it is not hosted in the United Arab Emirates, and the Provider makes no UAE data-residency commitment. The primary region in which Customer Content is stored is recorded in the Agreement particulars and is confirmed in writing by the Provider on request. The Provider shall notify Enterprise customers before any change to that region. Customer-controlled region selection may be agreed in an Order Form where the Provider is able to support it.

11.10 Worker health and fitness data. Where Customer Content includes health, fitness-to-work, medical, injury or rehabilitation information about workers, the Parties shall apply heightened protection: access restricted to named authorised personnel, purpose limitation to the Evaluation Purpose, and no use for any other purpose. The Customer confirms that it has a lawful basis for uploading such information.

12. AI-assisted features

12.1 Optional. The AI-Assisted Features are optional and may be disabled for the Evaluation Workspace at any time by the Customer's administrator. Every core workflow — controlled documents, permits, inspections, incidents and CAPA, MSRA/RAMS, training, subcontractor compliance, KPIs and audit evidence — works fully with AI disabled.

12.2 Draft only. AI output is a drafting aid and a starting point. It is not an authority decision, not a competent-person sign-off and not a substitute for professional judgement. Before any AI-assisted content is used on site, shared with a subcontractor, filed as evidence or submitted to a regulator, it must be reviewed and approved by a person with the competence and authority for the Customer's project.

12.3 No regulatory reliance. The Customer shall not rely on an AI-Assisted Feature's interpretation of a statute, code of practice or authority requirement. AI output must be verified against the Customer's approved procedures, the applicable legal references and the requirements of the relevant UAE authority.

12.4 No model training on Customer Content. The Provider does not use Customer Content to train, fine-tune or otherwise improve any third-party foundation model, and does not permit a Third-Party AI Provider to retain inputs for its own model training.

12.5 Third-Party AI Providers. Only the inputs required to answer a specific request are sent to a Third-Party AI Provider, for that request only. The Customer shall not submit

special category or sensitive data to an AI-Assisted Feature unless the Provider has confirmed in writing that the feature is enabled for that data.

12.6 Allowances. AI-Assisted Features consume AI Actions from the shared monthly allowance recorded in the Agreement particulars. Where the Customer is on a paid subscription, additional actions are charged at the published overage rate. Where the evaluation is provided at no charge, the Provider shall notify the Customer's administrator when the allowance is close to being exhausted and shall not charge an overage unless the Order Form permits it.

12.7 Accuracy. The Provider does not warrant the accuracy, completeness or suitability of AI output. AI output may misinterpret project details, omit context, or contain outdated or incorrect references. Clause 19.5 applies.

12.8 Reporting concerns. The Customer may report an incorrect, unsafe or misleading AI output to info@sitesafetyuae.com. The Provider reviews such reports and uses them to improve prompts, safeguards and guidance.

13. Customer Content and intellectual property

13.1 Customer ownership. The Customer retains all rights, title and interest in Customer Content. Nothing in this Agreement transfers ownership of Customer Content to the Provider.

13.2 Licence to the Provider. The Customer grants the Provider a limited, non-exclusive, worldwide, royalty-free licence to host, store, process, transmit, display, back up and otherwise use Customer Content solely to provide, secure, support and improve the Service, and to comply with law. The licence ends when the Customer Content is deleted in accordance with clause 11.6, except for copies in backups that expire on their own cycle.

13.3 Provider intellectual property. The Provider and its licensors retain all rights in the Service, including the software, architecture, data models, templates, authority report layouts, documentation, AI prompts and any improvement or derivative of them. No rights are granted except as expressly set out in this Agreement.

13.4 Feedback. The Customer grants the Provider a perpetual, royalty-free licence to use any feedback, suggestion or idea it provides about the Service, provided that the Provider does not identify the Customer as the source without its consent.

13.5 Aggregated data. The Provider may create aggregated and de-identified statistics about the use and performance of the Service, provided that the statistics do not identify the Customer, its Users, its sites or any individual, and are not used to re-identify any person.

13.6 Templates and authority content. The templates, checklists and authority report layouts supplied with the Service are provided as drafting aids. The Customer is responsible for confirming that any document it submits to an authority meets that authority's current requirements.

14. Confidentiality

14.1 Mutual Non-Disclosure Agreement. Where the Parties have signed a Mutual Non-Disclosure Agreement, it governs the exchange of Confidential Information in connection with this Agreement and prevails over this clause 14.

14.2 Fallback confidentiality terms. Where no Mutual Non-Disclosure Agreement is in force, each Party shall keep confidential all information disclosed by the other Party in connection with this Agreement that is identified as confidential or that a reasonable person would understand to be confidential from its nature or the circumstances of disclosure, shall use it only for the purposes of this Agreement, and shall not disclose it except to its personnel and professional advisers who need to know it and are bound by equivalent obligations. These obligations do not apply to information that is or becomes public other than through a breach, was lawfully held before disclosure, is lawfully obtained from a third party, or is independently developed. They continue for three (3) years after disclosure, and for so long as information remains a trade secret.

14.3 Compelled disclosure. A Party may disclose Confidential Information to the extent required by law, regulation or a competent authority, provided that it gives the other Party prompt notice where lawfully able to do so and discloses only the minimum required.

14.4 Publicity. Neither Party shall issue a press release, public statement, customer reference, case study or logo use referring to the other Party or to the evaluation without the other Party's prior written consent, except where disclosure is required by law.

15. Service changes and roadmap

15.1 Changes to the Service. The Provider may update, improve or modify the Service. The Provider shall not, during the Evaluation Period, materially reduce the core functionality of the modules recorded in Schedule A without the Customer's written agreement.

15.2 Deprecation. The Provider shall give the Customer at least ninety (90) days' written notice before discontinuing a material feature that the Customer is actively using, unless the discontinuation is required by law, by a third-party provider, or to address a security risk, in which case the Provider shall give as much notice as is reasonably practicable.

15.3 Preview and beta features. Preview, beta and early-access features are provided as-is, may be withdrawn or changed at any time, and are excluded from the Availability target in clause 7.1 and from the support targets in Schedule C unless the Provider states otherwise in writing.

15.4 Third-party services. The Service relies on third-party providers for hosting, database, authentication, storage, email delivery, payment processing and AI inference. The Provider is responsible for the selection of those providers and for the performance of

its obligations under this Agreement, and shall not be relieved of liability by a failure of a third-party provider that it has selected.

16. Suspension

16.1 Grounds for suspension. The Provider may suspend access to the Evaluation Workspace, in whole or in part, where: (a) the Customer is in material breach of clause 3.4 or of the acceptable use policy and has not remedied the breach within five (5) Business Days of written notice; (b) suspension is necessary to prevent or address a security incident, to protect the integrity of the Service or the data of other customers; or (c) suspension is required by law or by a competent authority.

16.2 Notice and proportionality. Where practicable, the Provider shall give the Customer's administrator notice before suspending access, and shall limit the suspension to what is necessary to address the ground for it. The Provider shall restore access promptly once the ground is resolved.

16.3 Suspension and service levels. Downtime caused by a suspension under clause 16.1(a) is Excluded Downtime. Downtime caused by a suspension under clause 16.1(b) or 16.1(c) is Excluded Downtime only where the Provider acted reasonably and the suspension was not caused by the Provider's own failure.

16.4 Extension for wrongful suspension. Where access is suspended under clause 16.1(b) or 16.1(c) for more than five (5) consecutive Business Days and the suspension was not caused by the Customer, the Evaluation Period is extended by the period of the suspension at no charge.

17. Term and termination

17.1 Term. This Agreement begins on the Effective Date and continues until the end of the Evaluation Period, unless terminated earlier under this clause 17 or extended under clause 5.2.

17.2 Termination for convenience. Either Party may terminate this Agreement at any time on ten (10) Business Days' written notice, without charge and without liability for the termination itself.

17.3 Termination for cause. Either Party may terminate this Agreement immediately on written notice where the other Party: (a) commits a material breach that is not capable of remedy; or (b) commits a material breach that is capable of remedy and fails to remedy it within fifteen (15) Business Days after written notice describing the breach.

17.4 Insolvency. Either Party may terminate this Agreement immediately on written notice where the other Party becomes insolvent, enters administration, liquidation or receivership, makes a general arrangement with its creditors, or ceases to carry on business.

17.5 Effect on other agreements. Termination of this Agreement does not terminate the Mutual Non-Disclosure Agreement, the Data Processing Agreement (to the extent it

governs Personal Data still held by the Provider) or any Order Form for a subscription that has already begun.

18. Consequences of termination

18.1 Cessation of access. On termination or expiry, the Customer's and its Users' right to access the Evaluation Workspace ends. The Provider shall disable access promptly, without prejudice to the Customer's rights under this clause 18.

18.2 Export window. For thirty (30) days after termination or expiry, the Provider shall make available to the Customer an export of Customer Content in a structured, commonly used and machine-readable format, together with the PDF exports the Customer has generated. The Customer should export any content it wishes to retain during this window, and is responsible for doing so.

18.3 Deletion. After the export window, the Provider shall delete or anonymise Customer Content and storage objects within thirty (30) days, excluding copies in backups, which expire on their own retention cycle of up to a further thirty (30) days. The Provider shall provide written confirmation of deletion on request.

18.4 Return of Confidential Information. Each Party shall return or destroy the other Party's Confidential Information in accordance with the Mutual Non-Disclosure Agreement, or, if none is in force, in accordance with clause 14.2, subject to any retention required by law.

18.5 Survival. Clauses 11, 13, 14, 18, 19, 20, 21, 25 and 26 survive termination or expiry, together with any other provision that by its nature is intended to survive.

18.6 Accrued rights. Termination or expiry does not affect any right or remedy that has already accrued, or the right to claim damages for a breach that occurred before termination.

19. Warranties and disclaimers

19.1 Mutual warranties. Each Party warrants that: (a) it has the legal capacity and authority to enter into and perform this Agreement; (b) the person signing on its behalf is duly authorised; and (c) entering into this Agreement does not breach any other agreement or obligation binding on it.

19.2 Service warranty. The Provider warrants that it shall provide the Service with reasonable skill and care, substantially in accordance with the documentation and the service levels in Schedule B and Schedule C, and that it shall maintain the security controls in Schedule D.

19.3 Evaluation disclaimer. Subject to clause 19.2, the Service is provided during the evaluation on an “as is” and “as available” basis. Preview and beta features, and any feature marked as experimental, are provided without warranty of any kind. The Provider does not warrant that the Service will be uninterrupted or error-free, or that every defect will be corrected.

19.4 No HSE warranty. The Provider does not warrant that use of the Service will achieve compliance with any law, code of practice, authority requirement, contract or standard, including ISO 45001, ADOSH-SF, the Dubai Municipality Code of Construction Safety Practice, Trakhees EHS Regulations or MOIAT requirements. The Provider does not certify the Customer's HSE management system and does not act as a competent person. The Customer remains responsible for workplace safety, statutory compliance and the approval of all site documentation.

19.5 AI disclaimer. The Provider does not warrant the accuracy, completeness, suitability or freedom from error of any AI-assisted output. All AI output must be reviewed and approved by a competent person before use, as required by clause 12.2.

19.6 Statutory rights. Nothing in this Agreement excludes, restricts or limits any warranty, right or remedy that cannot lawfully be excluded, restricted or limited.

20. Limitation of liability

20.1 Excluded losses. Neither Party is liable to the other for indirect or consequential loss, loss of profit, loss of revenue, loss of anticipated saving, loss of business or goodwill, loss or corruption of data (except where caused by the Provider's breach of clause 10 or clause 11, in which case the cost of restoring the data from the most recent backup is recoverable), or the cost of substitute services.

20.2 Cap. Subject to clause 20.3, each Party's total aggregate liability arising out of or in connection with this Agreement, whether in contract, tort (including negligence), breach of statutory duty or otherwise, is limited to: (a) where fees have been paid under this Agreement, the greater of the fees paid in the twelve (12) months before the event giving rise to the claim and USD 10,000; or (b) where the evaluation is provided at no charge, USD 10,000.

20.3 Unlimited liability. Nothing in this Agreement limits or excludes either Party's liability for: (a) death or personal injury caused by its negligence; (b) fraud or fraudulent misrepresentation; (c) breach of clause 3.4 (restrictions) or clause 14 (confidentiality); (d) infringement of the other Party's intellectual property rights; or (e) any liability that cannot lawfully be limited or excluded.

20.4 Service Credits. Service Credits are the Customer's sole financial remedy for a failure to meet the Availability target, as provided in clause 7.7. This clause 20.4 does not limit the Customer's rights for a breach of clause 10, clause 11 or clause 14.

20.5 Mitigation. Each Party shall take reasonable steps to mitigate any loss it suffers in connection with this Agreement, including by maintaining the independent copy of critical records required by clause 9.4.

20.6 Allocation of risk. The limitations in this clause 20 reflect the allocation of risk between the Parties, including the fact that the evaluation is provided at no charge or at a reduced charge, and are a material part of the basis on which the Parties have entered into this Agreement.

21. Indemnities

21.1 Provider indemnity. The Provider shall indemnify the Customer against direct losses, liabilities and reasonable legal costs awarded against the Customer in a third-party claim that the Service, used in accordance with this Agreement, infringes a United Arab Emirates or European Union registered intellectual property right. If such a claim is made or is reasonably likely, the Provider may, at its option, procure the right for the Customer to continue using the Service, modify the Service so that it is non-infringing while retaining equivalent functionality, or terminate this Agreement and refund any fees paid for the unused portion of the Evaluation Period. This indemnity does not apply to a claim arising from Customer Content, from a modification of the Service by the Customer, from use in combination with a product not supplied by the Provider, or from a version of the Service that the Provider has asked the Customer to stop using.

21.2 Customer indemnity. The Customer shall indemnify the Provider against direct losses, liabilities and reasonable legal costs arising from a third-party claim that Customer Content infringes a third party's intellectual property right, breaches a duty of confidence, or was uploaded in breach of applicable data protection law, provided that the Customer is responsible for that Content.

21.3 Procedure. The indemnified Party shall notify the indemnifying Party promptly, give it reasonable control of the defence and settlement, and provide reasonable assistance. The indemnifying Party shall not settle a claim in a way that admits liability on the part of the indemnified Party or imposes obligations on it without its written consent.

22. Compliance

22.1 General compliance. Each Party shall comply with all laws applicable to it in the United Arab Emirates and in any other jurisdiction in which it operates, including applicable data protection, cybercrime, anti-bribery, anti-money laundering and sanctions laws.

22.2 Anti-bribery. Neither Party shall offer, promise, give or accept any bribe, facilitation payment or other improper advantage in connection with this Agreement, and each Party shall have in place reasonable procedures to prevent such conduct.

22.3 Sanctions and export controls. Each Party represents and warrants that it is not the subject of any sanction or trade restriction that would prohibit it from performing this Agreement, and that it will not use the Service in breach of any applicable export control or sanctions regime.

22.4 Cooperation with authorities. Where an authority lawfully requires information from the Provider relating to the Customer, the Provider shall, where lawfully able to do so, notify the Customer before disclosing it and shall disclose only the minimum required.

23. Force majeure

23.1 Relief. Neither Party is liable for a failure or delay in performing an obligation under this Agreement (other than an obligation to pay money) caused by an event beyond its reasonable control, including war, civil unrest, terrorism, epidemic, natural disaster, flood, fire, failure of a public telecommunications network, or an act of government.

23.2 Exclusions. Force majeure does not include a failure of a third-party provider that the affected Party has selected and could reasonably have mitigated, a lack of funds, or a failure caused by the affected Party's own act or omission.

23.3 Notice and mitigation. The affected Party shall notify the other Party promptly, use reasonable efforts to mitigate the effect of the event, and resume performance as soon as reasonably practicable.

23.4 Extended force majeure. If a force majeure event continues for more than thirty (30) consecutive days, either Party may terminate this Agreement on written notice without liability for the termination itself.

24. Notices

24.1 Form and address. Notices under this Agreement shall be in writing and sent to the addresses or email addresses recorded in the Agreement particulars, or to such other address as a Party notifies in writing.

24.2 Deemed receipt. A notice is deemed received: (a) on delivery, if delivered by hand; (b) on the next Business Day, if sent by courier; and (c) at the time of transmission, if sent by email before 5.00 p.m. on a Business Day, or otherwise on the next Business Day, provided that no delivery failure notification is received.

24.3 Operational communications. Support tickets, incident notifications, maintenance notices and availability reports may be sent to the Customer's administrator and, where applicable, through in-app notification, and are not formal notices under this clause 24.

25. Governing law and dispute resolution

25.1 Governing law. This Agreement and any dispute or claim arising out of or in connection with it, including non-contractual disputes, are governed by the laws of the United Arab Emirates.

25.2 Jurisdiction. Subject to clause 25.4, the courts of the Emirate of Dubai have exclusive jurisdiction to settle any dispute arising out of or in connection with this Agreement.

25.3 Escalation. Before commencing proceedings, other than for urgent injunctive or interim relief, the Parties shall refer the dispute to a senior representative of each Party, who shall meet within ten (10) Business Days and use reasonable efforts to resolve it in good faith for a further period of twenty (20) Business Days. The Parties shall continue to perform their obligations during an escalation.

25.4 Interim relief. Nothing in this clause 25 prevents either Party from applying to any court of competent jurisdiction for interim, injunctive or protective relief to protect its Confidential Information or Customer Content.

25.5 Language of proceedings. This Agreement is in English. The Parties shall use reasonable efforts to have any proceedings and supporting documents conducted and produced in English where the forum permits. Any Arabic translation is for convenience only.

26. General provisions

26.1 Entire agreement. This Agreement, together with the documents listed in clause 2.1, is the entire agreement between the Parties in relation to its subject matter and supersedes all prior discussions, understandings and arrangements relating to it, except that a separately executed Order Form prevails to the extent provided in clause 2.3.

26.2 Variation. No variation of this Agreement is effective unless it is in writing and signed by an authorised representative of each Party. Electronic signature is permitted.

26.3 Waiver. No waiver of any provision is effective unless in writing and signed by the Party granting it. No failure or delay in exercising a right operates as a waiver of it.

26.4 Severability. If any provision of this Agreement is held to be invalid, illegal or unenforceable, that provision is severed or, where permitted, modified to the minimum extent necessary, and the remaining provisions continue in full force and effect.

26.5 Assignment. Neither Party may assign or transfer this Agreement without the prior written consent of the other Party, except to an Affiliate or to a successor in connection with a merger, reorganisation or sale of substantially all of its assets, on written notice to the other Party. For the purposes of this clause, “Affiliate” means an entity that controls, is controlled by, or is under common control with, a Party.

26.6 Subcontracting. The Provider may subcontract the performance of its obligations, including to the subprocessors listed under clause 11.4, provided that it remains responsible for the performance of this Agreement and for the acts and omissions of its subcontractors as if they were its own.

26.7 No partnership. Nothing in this Agreement creates a partnership, joint venture, agency, fiduciary or employment relationship between the Parties.

26.8 No third party rights. This Agreement does not create any right for any person who is not a Party, except that an Affiliate of a Party may enforce clause 3.4 as an intended beneficiary at that Party's discretion.

26.9 Relationship with the Terms of Service. Where this Agreement and the Terms of Service both address a matter, this Agreement prevails to the extent of any inconsistency, as provided in clause 2.3. The Terms of Service continue to apply to any use of the Service by an individual in a personal capacity.

26.10 Counterparts and electronic signature. This Agreement may be executed in counterparts, each of which is an original and all of which together constitute one

instrument. Electronic signatures and electronic records are valid and enforceable in accordance with Federal Decree-Law No. 46 of 2021.

26.11 Further assurance. Each Party shall, at its own cost, do all things reasonably necessary to give effect to this Agreement, including executing any further document reasonably requested by the other Party.

Execution

The Parties have executed this Agreement as of the Effective Date. By signing, each signatory confirms that they are duly authorised to bind the Party for which they sign, and the Customer confirms that it has read clause 2.4 (software-only licence) and clause 2.5 (shared responsibility).

For and on behalf of Site Safety LLC (trading as Site Safety UAE)	**For and on behalf of [Customer legal name]**
Signature:	Signature:
Name: [_____]	Name: [_____]
Title: [_____]	Title: [_____]
Date: [_____]	Date: [_____]
Email: [_____]	Email: [_____]

Schedule A — Evaluation scope and licensed modules

This schedule records what is included in the evaluation. Where an Order Form records a different scope, the Order Form prevails.

Element	Included in this evaluation	Notes
Evaluation Workspace	One logically separated workspace for the Customer	Company-email domain restriction may be enabled (clause 4.2)
Active project sites	[number] project sites	Enterprise supports unlimited sites; the evaluation is scoped to the sites recorded in the Agreement particulars
Named users	[number] named users	Access is per named individual; credentials must not be shared (clause 3.3)
Roles	Administrator, Manager, Supervisor, Viewer	Role-based permissions enforced on the server (clause 4.3)
Single sign-on	SAML SSO available on request	Automated SCIM provisioning is not currently offered (clause 4.4)
AI assist allowance	[number] AI Actions per calendar month	Shared across all AI-Assisted Features; AI may be disabled per workspace (clause 12.1)
Storage	[50 GB / 1 TB / other]	Additional storage may be purchased in blocks on a paid subscription
Data region	[primary region]	Confirmed in writing on request (clause 11.9)
Support tier	Enterprise — named account contact and priority escalation	See Schedule C
Availability target	99.5% monthly Uptime target Percentage	See Schedule B
Recovery objectives	As recorded in the Order Form	No universal RTO or RPO is published (clause 9.2)

Licensed modules

Module	Workflows included
Permits and high-risk work	Permit-to-work workflows, hot work, confined space, LOTO and SIMOPS permits, digital signature, hazard libraries, conflict detection, closeout QA and high-risk permit alerting.
Inspections, incidents and observations	Daily inspections, near-miss and observation capture with photo evidence, corrective and preventive action, lessons learned and management of change.
Controlled documents and MSRA/RAMS	Versioned method statements, risk assessments, certificates, policies and inductions, with expiry tracking, acknowledgements and a full audit trail.
People, training and subcontractors	Personnel register, training matrix, gate QR passes, induction records and subcontractor compliance status.

Reporting and audit evidence	Leading and lagging KPIs including TRIR, management review packs, and one-click evidence packs aligned to ISO 45001.
Awareness library	Bilingual awareness modules, toolbox talks and induction material.
UAE authority report templates	Report templates aligned to ADOSH-SF (formerly OSHAD), the Dubai Municipality Code of Construction Safety Practice and Trakhees EHS Regulations. The full suite, including MOIAT and Tasneef, and the custom report builder, are available on the Enterprise Plan.
AI-Assisted Features	MSRA drafting from the hazard library, incident root-cause suggestions, document review, warning-letter assistance and incident-photo hazard classification. Optional and subject to clause 12.

Schedule B — Service Level Agreement

This schedule sets the Availability target, the measurement method, the exclusions and the Service Credit remedy for the evaluation.

B1. Availability target

Metric	Target	Measurement period
Uptime Percentage	99.5%	Each calendar month
Maximum Downtime implied	216 minutes in a 30-day month; varies with month length	Excluding Excluded Downtime
Measurement source	Automated monitoring against the Provider's public health endpoint, with automated outage alerting	Continuous
Reporting	Monthly availability summary on request (clause 7.6)	Within 5 Business Days of month end

B2. Measurement and calculation

Uptime Percentage is calculated for each calendar month as: (total minutes in the month − Downtime minutes) ÷ (total minutes in the month) × 100, expressed to two decimal places.

Term	How it is treated
Core Service	Sign-in, the HSE dashboard, and the create, read and update operations for permits, inspections, incidents, documents, people and reports. The core Service does not include preview or beta features, AI-Assisted Features, notification delivery, PDF generation queues, or third-party services outside the Provider's control.
Downtime	Any period during which the core Service is unavailable to the Customer, other than Excluded Downtime. Downtime begins when the Provider's monitoring records a failure and ends when the core Service is available again.
Partial degradation	A period during which the core Service is available but a material workflow is substantially unusable is treated as Downtime for the affected workflow, weighted at fifty per cent (50%) unless the Parties agree otherwise. Repeated degradation of the same workflow in the same month is treated as full Downtime.
Customer-side issues	Unavailability caused by the Customer's own network, devices, browser configuration or identity provider is not Downtime.

B3. Excluded Downtime

Exclusion	Conditions
Scheduled Maintenance Window	Notice of at least 72 hours to the Customer's administrator where Downtime is expected; carried out within the window defined in B4.
Emergency maintenance	Carried out to protect security, integrity or stability; notice as soon as

	reasonably practicable; not recurring and reasonably avoidable.
Suspension under clause 16.1(a)	Suspension for the Customer's material breach of clause 3.4 or the acceptable use policy.
Force majeure	An event within clause 23 that affects the Service.
Customer or third-party act	An act or omission of the Customer, its Users, or a third party outside the Provider's control, including a failure of the Customer's identity provider.
Public internet	Failure of a public telecommunications network or internet routing outside the Provider's infrastructure.

B4. Maintenance windows

Item	Standard position
Standard Scheduled Maintenance Window	Sundays 02:00–05:00 GST, and such other windows as the Parties agree in the Order Form
Notice for a window expected to cause Downtime	At least 72 hours to the Customer's administrator
Maximum planned Downtime in a window	Three (3) hours unless otherwise agreed
Emergency maintenance	At any time, with notice as soon as reasonably practicable
Notification channel	Email to the Customer's administrator, and in-app notice where available

B5. Service Credits

Where the Uptime Percentage in a calendar month is below the target in clause 7.1, the Customer is entitled to the following Service Credit. During a no-charge evaluation, the Service Credit is taken as an extension of the Evaluation Period at no cost, calculated on the same percentages applied to the number of days in the affected month.

Uptime Percentage in the month	Service Credit	Evaluation extension
99.50% or above	None	None
99.00% to 99.49%	10% of the monthly fee	4 days
98.00% to 98.99%	15% of the monthly fee	5 days
95.00% to 97.99%	25% of the monthly fee	8 days
Below 95.00%	30% of the monthly fee	10 days

Service Credit terms	Position
Cap	The total Service Credit in any twelve-month period will not exceed 30% of the fees payable for that period. During a no-charge evaluation, the aggregate extension will not exceed 30 days.
Sole remedy	Service Credits are the sole financial remedy for a failure to meet the Availability target (clauses 7.7 and 20.4).

Claim procedure	The Customer may claim a Service Credit within thirty (30) days of the end of the affected month by submitting the information in Schedule E to info@sitesafetyuae.com. The Provider shall confirm or dispute the claim within ten (10) Business Days.
Evidence	The Provider shall provide the measured Uptime Percentage for the affected month on request, and shall not withhold the availability report on the basis that a claim has not been made.
Application	On a paid subscription, the credit is applied to the next invoice. During a no-charge evaluation, the Evaluation Period is extended by the number of days in the table above.

Schedule C — Support, severity and escalation

C1. Severity levels

Level	Definition	Examples
S1 — Outage	The core Service is unavailable, or a critical workflow cannot be used at all, and there is no workaround. Safety-critical data capture is prevented.	Cannot sign in; permits cannot be raised or closed; incident reporting unavailable; platform returning errors for all users.
S2 — Major	A material function is unavailable or materially degraded, or a significant number of users are affected, and only a limited or inconvenient workaround exists.	Report exports failing; notifications not sending; one site or module inaccessible; AI-Assisted Features failing.
S3 — Minor or question	A non-critical defect, a cosmetic issue, a single-user problem, or a product, configuration or billing question.	Display or formatting issue; a single user's permission problem; how-to question; request for clarification of an authority template.

C2. Response and resolution targets

Level	Acknowledgement	Substantive response	Resolution target
S1 — Outage	4 hours	Same Business Day	Best-efforts resolution; updates at least every 4 hours until resolved
S2 — Major	1 UAE Business Day	2 UAE Business Days	Most issues resolved within 48 hours of acknowledgement
S3 — Minor or question	2 UAE Business Days	5 UAE Business Days	Resolved or scheduled within 10 UAE Business Days

Where a fix requires a change to the software, the Provider shall confirm its diagnosis within the target period, provide a workaround where one exists, and keep the Customer updated until the fix ships. The published Support SLA and response-time policy (v1.2) sets the same Targets for the Enterprise plan.

C3. Support scope

Included	Not included
Defect reports and platform outages	On-site consulting, external audits or classroom training
Account, access, billing and invitation issues	Regulatory representation or submissions on the Customer's behalf
Product questions and guided setup help	Custom development outside the published roadmap
Clarification of the Provider's UAE authority report templates	Preparation of bespoke documents beyond what the Service generates

Guidance on configuration, roles and data import	A 24-hour telephone hotline — support is email-first

C4. Support hours and channels

Item	Position
Support Hours	Sunday to Thursday, 09:00–18:00 GST, excluding public holidays in the United Arab Emirates
Outside Support Hours	S1 incidents are monitored on a best-efforts basis, including weekends
Primary channel	Email to info@sitesafetyuae.com
Secondary channel	In-app “Report an issue”, which is triaged first
Named account contact	Provided to the Customer's administrator at onboarding
Language	English

C5. Escalation path

Stage	When it applies	Who is involved	Target
1 — Support	On raising a ticket	Provider support (founder-led)	Per C2
2 — Account escalation	An S1 or S2 is unresolved beyond its target, or the Customer disputes a Severity Level	Named account contact	1 UAE Business Day
3 — Founding team	An S1 is unresolved beyond 24 hours, or an escalation at stage 2 is not resolved	Founding team	Same Business Day
4 — Contractual escalation	The dispute concerns the interpretation of this Agreement	Senior representatives of each Party (clause 25.3)	Meeting within 10 Business Days

Schedule D — Security controls and shared responsibility

D1. Controls in place

Control	Position
Encryption in transit	All traffic served over HTTPS (TLS).
Encryption at rest	Data stored on managed PostgreSQL with provider-managed encryption at rest.
Row-level access control	Every record is scoped to the Customer's organisation and site. Row-level security policies are enforced in the database, not only in the interface.
Role-based permissions	Administrator, Manager, Supervisor and Viewer roles, stored separately from user profiles and checked on the server.
Company-email restriction	Workspace access can be restricted to the Customer's email domain; invitations and password resets use verified email flows.
Private document storage	Uploaded documents and photos are held in private buckets and accessed through short-lived signed URLs. No public links.
Audit trail	Document versions, permit signatures, acknowledgements, exports and administrative actions are recorded with user, timestamp and context, and can be exported.
Multi-factor authentication	Available and optional for user accounts; enabled on request for the Customer's administrators.
Password controls	Passwords are never stored in plain text; checks are run against known-compromised passwords.
Vulnerability reporting	Reports acknowledged within two (2) UAE Business Days; see clause 10.4.
Monitoring	Continuous uptime monitoring, automated outage alerting and a public health endpoint.

D2. Controls not in place at the Effective Date

The Provider states these plainly rather than implying otherwise. They are material to the Customer's risk assessment and are repeated in clause 10.2.

Not in place	Position
ISO 27001 / SOC 2 certification	Not held. The Provider does not claim certification of compliance.
Independent penetration test	Not completed at the Effective Date. Automated dependency and platform security scanning runs against every release.
SCIM directory provisioning	Not offered. User lifecycle is managed by the Customer's workspace administrators.
Customer-controlled region selection	Not currently offered. The primary region is confirmed in writing and the Customer is notified before a change (clause 11.9).
Universal RTO / RPO	Not published. Recovery objectives are agreed per Enterprise contract

	(clause 9.2).
On-site audit rights	Not offered during an evaluation. Assurance is documentation-based (clause 10.7).

D3. Shared responsibility

R = responsible, A = accountable, C = consulted, I = informed. The Provider is accountable for the platform; the Customer is accountable for its own HSE management system and for how the platform is used on its projects.

Activity	Provider	Customer
Platform availability, monitoring and incident response	A / R	I
Backup of the managed database and restore of Customer Content	A / R	I
Configuration of the Evaluation Workspace, sites and templates	C	A / R
Creation and deactivation of user accounts and role assignment	C / I	A / R
Off-boarding leavers and reviewing access periodically	I	A / R
Accuracy, completeness and lawfulness of Customer Content	I	A / R
Lawful basis for uploading worker, health and personal data	C	A / R
HSE decisions, permits, inspections, approvals and authority submissions	I	A / R
Review and approval of AI-assisted output before use	C / I	A / R
Applying security patches to the hosted Service	A / R	I
Security of the Customer's own devices, network and identity provider	I	A / R
Responding to data subject requests relating to Customer Content	R (assist)	A
Notifying a personal data breach to the Customer	A / R	I
Notifying a personal data breach to a regulator or data subject	C	A / R
Maintaining an independent copy of records the Customer must retain	I	A / R
Exporting Customer Content before the end of the Evaluation Period	R (facilitate)	A
Deletion of Customer Content after the export window	A / R	I

Schedule E — Service credit claim

Complete this schedule and email it to info@sitesafetyuae.com within thirty (30) days of the end of the affected month. The Provider shall confirm or dispute the claim within ten (10) Business Days.

Field	Entry
Customer legal name	[Customer legal name]
Evaluation reference	[SSUAE-EVAL-YYYY-###]
Customer administrator	[name and email address]
Affected calendar month	[Month YYYY]
Measured Uptime Percentage claimed	[xx.xx%]
Downtime events relied on	[date and time (GST), duration, affected workflow, ticket reference]
Whether a partial-degradation weighting is claimed	[Yes / No — if yes, describe the affected workflow]
Service Credit band claimed	[band from Schedule B5]
Remedy requested	[Evaluation Period extension / subscription credit on conversion]
Supporting evidence attached	[availability report, screenshots, ticket references, user reports]
Date of claim	[DD Month YYYY]

The Provider shall not reject a claim solely because the Customer did not monitor the Service itself, and shall not withhold the measured Uptime Percentage for the affected month.

Schedule F — Authorised users and notice details

The Customer shall complete this schedule before the first User is invited and shall keep it up to date. It may be updated by written notice to the Provider's administrator without varying any other provision of this Agreement.

Party	Notice email	Authorised signatory	Administrator
Site Safety LLC (trading as Site Safety UAE)	info@sitesafetyuae.com	Founder, Site Safety LLC	Founder, Site Safety LLC
[Customer legal name]	[name@company.com]	[name and title]	[name and title]

Named users

#	Full name	Company email	Role	Sites	Date	Date

					added	removed
1	[name]	[name@company.com]	[Administrator]	[all]	[date]	—
2	[name]	[name@company.com]	[Manager]	[site]	[date]	—
3	[name]	[name@company.com]	[Supervisor]	[site]	[date]	—
4	[name]	[name@company.com]	[Viewer]	[site]	[date]	—

Recovery objectives agreed for this evaluation

Objective	Agreed value
Recovery point objective (RPO)	[e.g. 1 hour]
Recovery time objective (RTO)	[e.g. 8 hours]
Restore test frequency	[e.g. annually, on request under clause 9.3]

End of Agreement