SAMPLE AGREEMENT

Cloud Service Agreement

This Agreement has 3 parts: (1) the Order Form and (2) the Key Terms, both of which are on the Cover Page, and (3) the Common Paper Cloud Service Standard Terms Version 1.1 posted at commonpaper.com/standards/cloud-service-agreement/1.1 ("**Standard Terms**"), which is incorporated by reference. If there is any inconsistency between the parts of the Agreement, the part listed earlier will control over the part listed later for that inconsistency. Capitalized and **highlighted** words have the meanings given on the Cover Page. However, if the Cover Page omits or does not define a highlighted word, the default meaning will be "none" or "not applicable" and the correlating clause, sentence, or section does not apply to this Agreement. All other capitalized words have the meanings given in the Standard Terms. A copy of the Standard Terms is attached for convenience only.

Order Form

The key business terms of this Agreement are as follows:

Cloud Service	The Cloud Service is: eesel AI allows you to create an AI that knows about your company knowledge and can instantly answer any question. eesel can integrate with your business workflows as an agent in chat tools, as a widget on your website or a customer service agent in a help desk tool to optimise business efficiency.
Subscription Start Date The date access to the Cloud Service starts	**Effective Date** (defined below)
Subscription Period Length of Cloud Service access	1 year(s)
Cloud Service Fees	[*Defined each time an agreement is sent*]
Payment Period Time frame for Customer to pay invoices	30 day(s) from **Customer's** receipt of invoice
Invoice Period How frequently Provider sends invoices	**Provider** will send invoices monthly
Auto-renewal	**Non-Renewal Notice Date:** at least 14 days before the end of the current **Subscription Period**.
SLA Service Level Agreement	Provider will use commercially reasonable efforts to provide and maintain the Cloud Service without excessive errors and interruptions. If Provider does not meet the SLA in two consecutive months or over three months in any 12-month period, then Customer may, as its only remedy, terminate this Order Form upon notice and receive a prorated refund of prepaid fees for the remainder of the Subscription Period.

Key Terms

The key legal terms of this Agreement are as follows:

Effective Date The date the Agreement starts	Date of last signature on this Cover Page
Governing Law	The laws of Delaware
Chosen Courts Jurisdiction or where disputes about the Agreement are filed	The courts (whether state, federal, or otherwise) located in Delaware

Covered Claims

Claims covered by indemnity obligations

Provider Covered Claims:

Any action, proceeding, or claim that the **Cloud Service**, when used by **Customer** according to the terms of the Agreement, violates, misappropriates, or otherwise infringes upon anyone else's intellectual property or other proprietary rights.

Customer Covered Claims:

Any action, proceeding, or claim that (1) the Customer Content, when used according to the terms of the Agreement, violates, misappropriates, or otherwise infringes upon anyone else's intellectual property or other proprietary rights; or (2) results from **Customer's** breach or alleged breach of Section 2.1 (Restrictions on Customer).

General Cap Amount

Limitation of liability amount for most claims

1.0 times the fees paid or payable by **Customer** to **Provider** in the 12 month period immediately preceding the claim

Additional Warranties

By Provider:

Security Measures. Provider hereby represents, warrants and covenants to Company that it will implement, maintain and will be in with any technical and/or organizational measures required to ensure the security and confidentiality of the Company's information, as outlined in Exhibit C (the "Security Measures").

Provider hereby represents, warrants and covenants to Company that the Deliverables (as such Deliverables are delivered by Provider) do not contain, and Provider will not insert into any Deliverable, any lock, dongle, clock, timer, counter, hardware key, copy protection feature, replication device, "virus" or "worm," as those terms are commonly used in the computer industry, or other software code that may (a) lock, disable, or erase any Deliverable, or any other software, programs, or data of Company (b) limit or prevent full use of or copying of the Deliverables as permitted under this Agreement, (c) harm or otherwise interfere with Company's servers or data processing hardware (including terminals, auxiliary storage, and communication and peripheral devices), or (d) require action or intervention by Provider or any other person to allow use of the Deliverables as permitted under this Agreement.

Insurance Minimums

Requirements for Provider's policies

Commercial general liability with a minimum limit for each occurrence of at least $1,000,000.00 and at least $2,000,000.00 in the aggregate.

Errors and omissions or professional liability with a minimum limit for each occurrence of at least $1,000,000.00 and at least $2,000,000.00 in the aggregate.

Cyber liability insurance with a minimum limit for each occurrence of at least $500,000.00 and at least $2,000,000.00 in the aggregate.

DPA

Data Processing Agreement

The following document is incorporated into this Agreement: **Attachment #1: eesel Inc, DPA 1.1** (PDF Document)

Security Policy

The following document is incorporated into this Agreement: **Attachment #2: eesel Inc, CSA - Security Measures (Exhibit A) - Public Copy** (PDF Document)

Provider and **Customer** have not changed the Standard Terms, except for the details on the Cover Page above. By signing this Cover Page, each party agrees to enter into this Agreement as of the Effective Date.

	PROVIDER: eesel, Inc	**CUSTOMER:**
Signature		
Print Name		
Title		
Notice Address	651 N Broad St Middletown, Delaware 19709 United States of America	
Date		

Cloud Service Agreement

1. Service

1.1 Access and Use. During the Subscription Period and subject to the Use Limitations , Customer may (a) access and use the Cloud Service; and (b) copy and use the included Software and Documentation only as needed to access and use the Cloud Service, in each case, for its internal business purposes and only if Customer complies with the terms of this Agreement.

1.2 Service Level. If there is an SLA and the Cloud Service does not meet the SLA , Provider will provide the remedies outlined in the SLA and will not be responsible for any other remedies. Any credits earned under the SLA will only apply to future invoices and expire if the Agreement ends. In any event, if the Cloud Service is temporarily unavailable for scheduled maintenance, for unscheduled emergency maintenance, or because of other causes beyond Provider's reasonable control, no SLA remedies will accrue. Provider will try to inform Customer before scheduled service disruptions through the Cloud Service or by email.

1.3 Support. During the Subscription Period , Provider will provide Technical Support as described in the Cover Page, if any.

1.4 User Accounts. Customer is responsible for all actions on Users' accounts and for Users' compliance with this Agreement. Customer and Users must protect the confidentiality of their passwords and login credentials. Customer will promptly notify Provider if it suspects or knows of any fraudulent activity with its accounts, passwords, or credentials, or if they become compromised.

1.5 Affiliates. If authorized in a Cover Page, individuals from Customer's Affiliates may access Customer's account as Users under Customer's Agreement and Customer will be responsible for its Affiliates' compliance with this Agreement. If a Customer Affiliate enters a separate Cover Page with Provider , the Customer's Affiliate creates a separate agreement between Provider and that Affiliate, where Provider's responsibility to the Affiliate is individual and separate from Customer and Customer is not responsible for its Affiliates' agreement.

1.6 Feedback and Usage Data. Customer may, but is not required to, give Provider Feedback, in which case Customer gives Feedback "AS IS". Provider may use all Feedback freely without any restriction or obligation. In addition, Provider may collect and analyze Usage Data, and Provider may freely use Usage Data to maintain, improve, and enhance Provider's products and services without restriction or obligation. However, Provider may only share Usage Data with others if the Usage Data is aggregated and does not identify Customer or Users.

1.7 Customer Content. Provider may copy, display, modify, and use Customer Content only as needed to provide and maintain the Product and related offerings. Customer is responsible for the accuracy and content of Customer Content.

2. Restrictions & Obligations

2.1 Restrictions on Customer.

a. Except as expressly permitted by this Agreement, Customer will not (and will not allow any anyone else to): (i) reverse engineer, decompile, or attempt to discover any source code or underlying ideas or algorithms of the Product (except to the extent Applicable Laws prohibit this restriction); (ii) provide, sell, transfer, sublicense, lend, distribute, rent, or otherwise allow others to access or use the Product; (iii) remove any proprietary notices or labels; (iv) copy, modify, or create derivative works of the Product; (v) conduct security or vulnerability tests on, interfere with the operation of, cause performance degradation of, or circumvent access restrictions of the Product; (vi) access accounts, information, data, or portions of the Product to which Customer does not have explicit authorization; (vii) use the Product to develop a competing service or product; (viii) use the Product with any High Risk Activities or with activity prohibited by Applicable Laws; (ix) use the Product to obtain unauthorized access to anyone else's networks or equipment; or (x) upload, submit, or otherwise make available to the Product any Customer Content to which Customer and Users do not have the proper rights.

b. Customer's use of the Product must comply with all Documentation and the Acceptable Use Policy , if any.

2.2 Suspension. If Customer (a) has an outstanding, undisputed balance on its account for more than 30 days after the Payment Period ; (b) breaches Section 2.1 (Restrictions on Customer); or (c) uses the Product in violation of the Agreement or in a way that materially and negatively impacts the Product or others, then Provider may temporarily suspend Customer's access to the Product with or without notice. However, Provider will try to inform Customer before suspending Customer's account when practical. Provider will reinstate Customer's access to the Product only if Customer resolves the underlying issue.

3. Professional Services

Provider will perform the Professional Services as detailed in a Cover Page, if any, and Customer will reasonably cooperate with Provider to allow the performance of Professional Services , including providing Customer Content as needed. Provider is not responsible for any inability to perform the Professional Services if Customer does not cooperate as reasonably requested.

4. Privacy & Security

4.1 Personal Data. Before submitting Personal Data governed by GDPR, Customer must enter into a data processing agreement with Provider . If the parties have a DPA , the terms of the DPA will control each party's rights and obligations as to Personal Data and the terms of the DPA will control in the event of any conflict with this Agreement.

4.2 Prohibited Data. Customer will not (and will not allow anyone else to) submit Prohibited Data to the Product unless authorized by the Cover Page.

4.3 Security. Provider will comply with the Security Policy , if any.

5. Payment & Taxes

5.1 Fees and Invoices. All fees are in U.S. Dollars and are exclusive of taxes. Except for the prorated refund of prepaid fees allowed with specific termination rights, fees are non-refundable. Provider will send invoices for fees applicable to the Product once per Invoice Period in advance starting on the Subscription

Start Date . Invoices for Professional Services may be sent monthly during performance of the Professional Services unless the Cover Page includes a different cadence.

5.2 Payment. Customer will pay Provider the fees and taxes in each invoice in U.S. Dollars within the Payment Period .

5.3 Taxes. Customer is responsible for all duties, taxes, and levies that apply to fees, including sales, use, VAT, GST, or withholding, that Provider itemizes and includes in an invoice. However, Customer is not responsible for Provider's income taxes.

5.4 Payment Dispute. If Customer has a good-faith disagreement about the amounts charged on an invoice, Customer must notify Provider about the dispute during the Payment Period for the invoice and must pay all undisputed amounts on time. The parties will work together to resolve the dispute within 15 days after the end of the Payment Period . If no resolution is agreed, each party may pursue any remedies available under the Agreement or Applicable Laws.

6. Term & Termination

6.1 Subscription Period. Each Order Form will start on the Subscription Start Date , continue for the Subscription Period , and automatically renew for additional Subscription Periods unless one party gives notice of non-renewal to the other party before the Non-Renewal Notice Date .

6.2 Agreement Term. This Agreement will start on the Effective Date and continue for the longer of one year or until all Subscription Periods have ended.

6.3 Termination. Either party may terminate this Agreement if the other party (a) fails to cure a material breach of the Agreement within 30 days after receiving notice of the breach; (b) materially breaches the Agreement in a manner that cannot be cured; (c) dissolves or stops conducting business without a successor; (d) makes an assignment for the benefit of creditors; or (e) becomes the debtor in insolvency, receivership, or bankruptcy proceedings that continue for more than 60 days. In addition, either party may terminate an affected Order Form if a Force Majeure Event prevents the Product from materially operating for 30 or more consecutive days, and Provider will pay to Customer a prorated refund of prepaid fees for the remainder of the Subscription Period . A party must notify the other of its reason for termination.

6.4 Effect of Termination. Termination of the Agreement will automatically terminate all Order Forms. Upon expiration or termination:

a. Customer will no longer have any right to use the Product, Technical Support , or Professional Services .

b. Upon Customer's request, Provider will delete Customer Content within 60 days.

c. Each Recipient will return or destroy Discloser's Confidential Information in its possession or control.

d. Provider will submit a final invoice for all outstanding fees accrued before termination and Customer will pay the invoice according to Section 5 (Payment & Taxes).

6.5 Survival.

a. The following sections will survive expiration or termination of the Agreement: Section 1.6 (Feedback and Usage Data), Section 2.1 (Restrictions on Customer), Section 5 (Payment & Taxes) for fees accrued or payable before expiration or termination, Section 6.4 (Effect of Termination), Section 6.5 (Survival), Section 7 (Representations & Warranties), Section 8 (Disclaimer of Warranties), Section 9 (Limitation of Liability), Section 10 (Indemnification), Section 11 (Insurance) for the time period specified, Section 12 (Confidentiality), Section 13 (Reservation of Rights), Section 14 (General Terms), Section 15 (Definitions), and the portions of a Cover Page referenced by these sections.

b. Each Recipient may retain Discloser's Confidential Information in accordance with its standard backup or record retention policies maintained in the ordinary course of business or as required by Applicable Laws, in which case Section 4 (Privacy & Security) and Section 12 (Confidentiality) will continue to apply to retained Confidential Information.

7. Representations & Warranties

7.1 Mutual. Each party represents and warrants to the other that: (a) it has the legal power and authority to enter into this Agreement; (b) it is duly organized, validly existing, and in good standing under the Applicable Laws of the jurisdiction of its origin; (c) it will comply with all Applicable Laws in performing its obligations or exercising its rights in this Agreement; and (d) it will comply with the Additional Warranties .

7.2 From Customer. Customer represents and warrants that it, all Users, and anyone submitting Customer Content each have and will continue to have all rights necessary to submit or make available Customer Content to the Product and to allow the use of Customer Content as described in the Agreement.

7.3 From Provider. Provider represents and warrants to Customer that (a) it will not materially reduce the general functionality of the Cloud Service during a Subscription Period ; and (b) it will perform Professional Services in a competent and professional manner.

7.4 Provider Warranty Remedy. If Provider breaches a warranty in Section 7.3, Customer must give Provider notice (with enough detail for Provider to understand or replicate the issue) within 45 days of discovering the issue. Within 45 days of receiving sufficient details of the warranty issue, Provider will attempt to restore the general functionality of the Cloud Service or reperform the Professional Services . If Provider cannot resolve the issue, Customer may terminate the affected Order Form and Provider will pay to Customer a prorated refund of prepaid fees for the remainder of the Subscription Period . Provider's restoration and reperformance obligations, and Customer's termination right, are Customer's only remedies if Provider does not meet the warranties in Section 7.3.

8. Disclaimer of Warranties

Provider makes no guarantees that the Product will always be safe, secure, or error-free, or that it will function without disruptions, delays, or imperfections. The warranties in Section 7.3 do not apply to any misuse or unauthorized modification of the Product, nor to any product or service provided by anyone other than Provider . Except for the warranties in Section 7, Provider and Customer each **disclaim all other warranties, whether express or implied, including the implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement.** These disclaimers apply to the maximum extent permitted by Applicable Laws.

9. Limitation of Liability

9.1 Liability Caps. **If there are Increased Claims , each party's total cumulative liability for the Increased Claims arising out of or relating to this Agreement will not be more than the Increased Cap Amount . Each party's total cumulative liability for all other claims arising out of or relating to this**

Agreement will not be more than the General Cap Amount .

9.2 Damages Waiver. **Each party's liability for any claim or liability arising out of or relating to this Agreement will be limited to the fullest extent permitted by Applicable Laws. Under no circumstances will either party be liable to the other for lost profits or revenues, or for consequential, special, indirect, exemplary, punitive, or incidental damages relating to this Agreement, even if the party is informed of the possibility of this type of damage in advance.**

9.3 Exceptions. The liability caps in Section 9.1 and the damages waiver in Section 9.2 do not apply to any Unlimited Claims . The damages waiver in Section 9.2 does not apply to any Increased Claims .

10. Indemnification

10.1 Protection by Provider. Provider will indemnify, defend, and hold harmless Customer from and against all Provider Covered Claims made by someone other than Customer , Customer's Affiliates, or Users, and all out-of-pocket damages, awards, settlements, costs, and expenses, including reasonable attorneys' fees and other legal expenses, that arise from the Provider Covered Claim .

10.2 Protection by Customer. Customer will indemnify, defend, and hold harmless Provider from and against all Customer Covered Claims made by someone other than Provider or its Affiliates, and all out-of-pocket damages, awards, settlements, costs, and expenses, including reasonable attorneys' fees and other legal expenses, that arise from the Customer Covered Claim .

10.3 Procedure. The Indemnifying Party's obligations in this section are contingent upon the Protected Party: (a) promptly notifying the Indemnifying Party of each Covered Claim for which it seeks protection; (b) providing reasonable assistance to the Indemnifying Party at the Indemnifying Party's expense; and (c) giving the Indemnifying Party sole control over the defense and settlement of each Covered Claim. A Protected Party may participate in a Covered Claim for which it seeks protection with its own attorneys only at its own expense. The Indemnifying Party may not agree to any settlement of a Covered Claim that contains an admission of fault or otherwise materially and adversely impacts the Protected Party without the prior written consent of the Protected Party.

10.4 Changes to Product. If required by settlement or court order, or if deemed reasonably necessary in response to a Provider Covered Claim , Provider may: (a) obtain the right for Customer to continue using the Product; (b) replace or modify the affected component of the Product without materially reducing the general functionality of the Product; or (c) if neither (a) nor (b) are reasonable, terminate the affected Order Form and issue a pro-rated refund of prepaid fees for the remainder of the Subscription Period .

10.5 Exclusions.

a. Provider's obligations as an Indemnifying Party will not apply to Provider Covered Claims that result from (i) modifications to the Product that were not authorized by Provider or that were made in compliance with Customer's instructions; (ii) unauthorized use of the Product, including use in violation of this Agreement; (iii) use of the Product in combination with items not provided by Provider ; or (iv) use of an old version of the Product where a newer release would avoid the Provider Covered Claim .

b. Customer's obligations as an Indemnifying Party will not apply to Customer Covered Claims that result from the unauthorized use of the Customer Content, including use in violation of this Agreement.

10.6 Exclusive Remedy. This Section 10 (Indemnification), together with any termination rights, describes each Protected Party's exclusive remedy and each Indemnifying Party's entire liability for a Covered Claim.

11. Insurance

During the Subscription Period and for six months after, Provider will carry commercial insurance policies with coverage limits that meet the Insurance Minimums , if any. Upon request, Provider will give Customer a certificate of insurance evidencing its insurance policies that meet the Insurance Minimums . Provider's insurance policies will not be considered as evidence of Provider's liability.

12. Confidentiality

12.1 Non-Use and Non-Disclosure. Unless otherwise authorized in the Agreement, Recipient will (a) only use Discloser's Confidential Information to fulfill its obligations or exercise its rights under this Agreement; and (b) not disclose Discloser's Confidential Information to anyone else. In addition, Recipient will protect Discloser's Confidential Information using at least the same protections Recipient uses for its own similar information but no less than a reasonable standard of care.

12.2 Exclusions. Confidential Information does not include information that (a) Recipient knew without any obligation of confidentiality before disclosure by Discloser; (b) is or becomes publicly known and generally available through no fault of Recipient; (c) Recipient receives under no obligation of confidentiality from someone else who is authorized to make the disclosure; or (d) Recipient independently developed without use of or reference to Discloser's Confidential Information.

12.3 Required Disclosures. Recipient may disclose Discloser's Confidential Information to the extent required by Applicable Laws if, unless prohibited by Applicable Laws, Recipient provides the Discloser reasonable advance notice of the required disclosure and reasonably cooperates, at the Discloser's expense, with the Discloser's efforts to obtain confidential treatment for the Confidential Information.

12.4 Permitted Disclosures. Recipient may disclose Discloser's Confidential Information to Users, employees, advisors, contractors, and representatives who each have a need to know the Confidential Information, but only if the person or entity is bound by confidentiality obligations at least as protective as those in this Section 12 and Recipient remains responsible for everyone's compliance with the terms of this Section 12.

13. Reservation of Rights

Except for the limited license to copy and use Software and Documentation in Section 1.1 (Access and Use), Provider retains all right, title, and interest in and to the Product, whether developed before or after the Effective Date . Except for the limited rights in Section 1.7 (Customer Content), Customer retains all right, title, and interest in and to the Customer Content.

14. General Terms

14.1 Entire Agreement. This Agreement is the only agreement between the parties about its subject and this Agreement supersedes all prior or contemporaneous statements (whether in writing or not) about its subject. Provider expressly rejects any terms included in Customer's purchase order or similar document, which may only be used for accounting or administrative purposes.

14.2 Modifications, Severability, and Waiver. Any waiver, modification, or change to the Agreement must be in writing and signed or electronically accepted by each party. However, Provider may update Technical Support , the SLA , the Security Policy , or the Acceptable Use Policy by giving Customer 30 days prior notice. During the 30-day notice period, Customer may terminate the Agreement or affected Order Form upon notice if the update is a material reduction from the prior version and Provider cannot reasonably restore the prior version or a comparable alternative. If any term of this Agreement is determined to be invalid or unenforceable by a relevant court or governing body, the remaining terms of this Agreement will remain in full force and effect. The failure of a party to enforce a term or to exercise an option or right in this Agreement will not constitute a waiver by that party of the term, option, or right.

14.3 Governing Law and Chosen Courts. The Governing Law will govern all interpretations and disputes about this Agreement, without regard to its conflict of laws provisions. The parties will bring any legal suit, action, or proceeding about this Agreement in the Chosen Courts and each party irrevocably submits to the exclusive jurisdiction of the Chosen Courts .

14.4 Injunctive Relief. Despite Section 14.3 (Governing Law and Chosen Courts), a breach of Section 12 (Confidentiality) or the violation of a party's intellectual property rights may cause irreparable harm for which monetary damages cannot adequately compensate. As a result, upon the actual or threatened breach of Section 12 (Confidentiality) or violation of a party's intellectual property rights, the non-breaching or non-violating party may seek appropriate equitable relief, including an injunction, in any court of competent jurisdiction without the need to post a bond and without limiting its other rights or remedies.

14.5 Non-Exhaustive Remedies. Except where the Agreement provides for an exclusive remedy, seeking or exercising a remedy does not limit the other rights or remedies available to a party.

14.6 Assignment. Neither party may assign any rights or obligations under this Agreement without the prior written consent of the other party. However, either party may assign this Agreement upon notice if the assigning party undergoes a merger, change of control, reorganization, or sale of all or substantially all its equity, business, or assets to which this Agreement relates. Any attempted but non-permitted assignment is void. This Agreement will be binding upon and inure to the benefit of the parties and their permitted successors and assigns.

14.7 No Publicity. Neither party may publicly announce the existence of this Agreement without the prior written approval of the other party.

14.8 Notices. Any notice, request, or approval about the Agreement must be in writing and sent to the Notice Address . Notices will be deemed given (a) upon confirmed delivery if by email, registered or certified mail, or personal delivery; or (b) two days after mailing if by overnight commercial delivery.

14.9 Independent Contractors. The parties are independent contractors, not agents, partners, or joint venturers. Neither party is authorized to bind the other to any liability or obligation.

14.10 No Third-Party Beneficiary. There are no third-party beneficiaries of this Agreement.

14.11 Force Majeure. Neither party will be liable for a delay or failure to perform its obligations of this Agreement if caused by a Force Majeure Event. However, this section does not excuse Customer's obligations to pay fees.

14.12 Export Controls. Customer may not remove or export from the United States or allow the export or re-export of the Product or any related technology or materials in violation of any restrictions, laws, or regulations of the United States Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, or any other United States or foreign agency or authority.

14.13 Government Rights. The Cloud Service and Software are deemed "commercial items" or "commercial computer software" according to FAR section 12.212 and DFAR section 227.7202, and the Documentation is "commercial computer software documentation" according to DFAR section 252.227-7014(a)(1) and (5). Any use, modification, reproduction, release, performance, display, or disclosure of the Product by the U.S. Government will be governed solely by the terms of this Agreement and all other use is prohibited.

14.14 Anti-Bribery. Neither party will take any action that would be a violation of any Applicable Laws that prohibit the offering, giving, promising to offer or give, or receiving, directly or indirectly, money or anything of value to any third party to assist Provider or Customer in retaining or obtaining business. Examples of these kinds of laws include the U.S. Foreign Corrupt Practices Act and the UK Bribery Act 2010.

14.15 Titles and Interpretation. Section titles are for convenience and reference only. All uses of "including" and similar phrases are non-exhaustive and without limitation. The United Nations Convention for the International Sale of Goods and the Uniform Computer Information Transaction Act do not apply to this Agreement.

14.16 Signature. This Agreement may be signed in counterparts, including by electronic copies or acceptance mechanism. Each copy will be deemed an original and all copies, when taken together, will be the same agreement.

15. Definitions

15.1 **"Affiliate"** means an entity that, directly or indirectly, controls, is under the control of, or is under common control with a party, where control means having more than fifty percent (50%) of the voting stock or other ownership interest.

15.2 **"Agreement"** means these Standard Terms, together with the Cover Pages between Provider and Customer that include or reference a single set of Key Terms and the policies and documents referenced in or attached to those Cover Pages.

15.3 **"Applicable Data Protection Laws"** means the Applicable Laws that govern how the Cloud Service may process or use an individual's personal information, personal data, personally identifiable information, or other similar term.

15.4 **"Applicable Laws"** means the laws, rules, regulations, court orders, and other binding requirements of a relevant government authority that apply to or govern Provider or Customer .

15.5 **"Cloud Service"** means the product described in an Order Form.

15.6 **"Confidential Information"** means information in any form disclosed by or on behalf of a Discloser, including before the Effective Date , to a Recipient in connection with this Agreement that (a) the Discloser identifies as "confidential", "proprietary", or the like; or (b) should be reasonably understood as confidential or proprietary due to its nature and the circumstances of its disclosure. Confidential Information includes the existence of this Agreement and the information on each Cover Page. Customer's Confidential Information includes non-public Customer Content and Provider's Confidential Information includes non-public information about the Product.

15.7 **"Cover Page"** means a document that is signed or electronically accepted by the parties that incorporates these Standard Terms, identifies Provider and Customer , and may include an Order Form, Key Terms, or both.

15.8 **“Covered Claim”** means either a **Provider Covered Claim** or **Customer Covered Claim** .

15.9 **“Customer Content”** means data, information, or materials submitted by or on behalf of **Customer** or Users to the Product, but excludes Feedback.

15.10 **“Discloser”** means a party to this Agreement when the party is providing or disclosing Confidential Information to the other party.

15.11 **“Documentation”** means the usage manuals and instructional materials for the Cloud Service or Software that are made available by **Provider** .

15.12 **“Feedback”** means suggestions, feedback, or comments about the Product or related offerings.

15.13 **“Force Majeure Event”** means an unforeseen event outside a party’s reasonable control where the affected party took reasonable measures to avoid or mitigate the impacts of the event. Examples of these kinds of events include unpredicted natural disaster like a major earthquake, war, pandemic, riot, act of terrorism, or public utility or internet failure.

15.14 **“GDPR”** means European Union Regulation 2016/679 as implemented by local law in the relevant European Union member nation, and by section 3 of the United Kingdom’s European Union (Withdrawal) Act of 2018 in the United Kingdom.

15.15 **“High Risk Activity”** means any situation where the use or failure of the Product could be reasonably expected to lead to death, bodily injury, or environmental damage. Examples include full or partial autonomous vehicle technology, medical life-support technology, emergency response services, nuclear facilities operation, and air traffic control.

15.16 **“Indemnifying Party”** means a party to this Agreement when the party is providing protection for a particular Covered Claim.

15.17 **“Key Terms”** means the portion of a Cover Page that includes the key legal details and definitions for this Agreement that are not defined in the Standard Terms. The Key Terms may include details about Covered Claims, set the **Governing Law** , or contain other details about this Agreement.

15.18 **“Order Form”** means the portion of a Cover Page that includes the key business details and definitions for this Agreement that are not defined in the Standard Terms. An Order Form may include details about the level of access and use granted to the Cloud Service, nature and timing of **Professional Services** , extent of **Technical Support** , or other details about the Product.

15.19 **“Personal Data”** will have the meaning(s) set forth in the Applicable Data Protection Laws for personal information, personal data, personally identifiable information, or other similar term.

15.20 **“Product”** means the Cloud Service, Software, and Documentation.

15.21 **“Prohibited Data”** means (a) patient, medical, or other protected health information regulated by the Health Insurance Portability and Accountability Act; (b) credit, debit, bank account, or other financial account numbers; (c) social security numbers, driver’s license numbers, or other unique and private government ID numbers; (d) special categories of data as defined in the GDPR; and (e) other similar categories of sensitive information as set forth in the Applicable Data Protection Laws.

15.22 **“Protected Party”** means a party to this Agreement when the party is receiving the benefit of protection for a particular Covered Claim.

15.23 **“Recipient”** means a party to this Agreement when the party receives Confidential Information from the other party.

15.24 **“Software”** means the client-side software or applications made available by **Provider** for **Customer** to install, download (whether onto a machine or in a browser), or execute as part of the Product.

15.25 **“Usage Data”** means data and information about the provision, use, and performance of the Product and related offerings based on **Customer’s** or User’s use of the Product.

15.26 **“User”** means any individual who uses the Product on **Customer’s** behalf or through **Customer’s** account.

SAMPLE AGREEMENT

Data Processing Agreement

This DPA has 2 parts: (1) the Key Terms on this Cover Page and (2) the Common Paper DPA Standard Terms Version 1.0 posted at commonpaper.com/standards/data-processing-agreement/1.0 (**"DPA Standard Terms"**), which is incorporated by reference. If there is any inconsistency between the parts of the DPA, the Cover Page will control over the DPA Standard Terms. Capitalized and **highlighted** words have the meanings given on the Cover Page. However, if the Cover Page omits or does not define a highlighted word, the default meaning will be "none" or "not applicable" and the correlating clause, sentence, or section does not apply to this Agreement. All other capitalized words have the meanings given in the DPA Standard Terms or the **Agreement**. A copy of the DPA Standard Terms is attached for convenience only.

Agreement	Reference to sales contract will be set when sending agreement
Approved Subprocessors	https://docs.google.com/document/d/18ja94HSiZPIaOypZVhDO2raYEtFNIXSXjQYInjzncTE
Provider Security Contact	pat@eesel.app
Security Policy	Security Policy available at: https://docs.google.com/document/d/14NYCJdNRLuK11cW8CqtHvSa_PTcleoEwBRWmdOo3OIM/edit?usp=sharing
Changes to the agreement	
Service Provider Relationship	To the extent California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq ("CCPA") applies, the parties acknowledge and agree that Provider is a service provider and is receiving Personal Data from Customer to provide the Service as agreed in the Agreement and detailed below (*see* Nature and Purpose of Processing), which constitutes a limited and specified business purpose. Provider will not sell or share any Personal Data provided by Customer under the Agreement. In addition, Provider will not retain, use, or disclose any Personal Data provided by Customer under the Agreement except as necessary for providing the Service for Customer, as stated in the Agreement, or as permitted by Applicable Data Protection Laws. Provider certifies that it understands the restrictions of this paragraph and will comply with all Applicable Data Protection Laws. Provider will notify Customer if it can no longer meet its obligations under the CCPA.
Restricted Transfers	
Governing Member State	EEA Transfers: Netherlands UK Transfers: England and Wales
Annex I(A) List of Parties	
Data Exporter	**Name:** the **Customer** signing this DPA **Activities relevant to transfer:** See Annex 1(B) **Role:** Controller
Data Importer	**Name:** the **Provider** signing this DPA **Contact person:** Amogh Sarda, CEO, Co-Founder **Address:** 651 N Broad St, Middletown, Delaware 19709, USA **Activities relevant to transfer:** See Annex 1(B) **Role:** Processor
Annex I(B) Description of Transfer and Processing Activities	
Service	**The Service is:** eesel AI allows you to create an AI that knows about your company knowledge and can instantly answer any question. eesel can integrate with your business workflows as an agent on Slack, as a widget on your website or a customer service agent in a help desk tool to optimise business efficiency.
Categories of Data Subjects	**Customer's** end users or customers **Customer's** employees

Categories of Personal Data	User activity and analysis such as device information or IP address - User generated content data explicitly provided to the Data Processor - Incidental contact information if it appears within user generated content data provided to the Provider.
Special Category Data Is special category data (as defined in Article 9 of the GDPR) Processed?	No
Frequency of Transfer	Continuous
Nature and Purpose of Processing	Receiving data, including collection, accessing, retrieval, recording, and data entry Holding data, including storage, organization, and structuring Using data, including analysis, consultation, testing, automated decision making, and profiling Updating data, including correcting, adaption, alteration, alignment, and combination Protecting data, including restricting, encrypting, and security testing Sharing data, including disclosure, dissemination, allowing access, or otherwise making available Returning data to the data exporter or data subject Erasing data, including destruction and deletion
Duration of Processing	**Provider** will process Customer Personal Data as long as required (i) to conduct the Processing activities instructed in Section 2.2(a)-(d) of the Standard Terms; or (ii) by Applicable Laws.

Annex I(C)

Competent Supervisory Authority	The supervisory authority will be the supervisory authority of the data exporter, as determined in accordance with Clause 13 of the EEA SCCs or the relevant provision of the UK Addendum.

Annex II

Technical and Organizational Security Measures	See **Security Policy**

Provider and Customer have not changed the Standard Terms, except for the details on the Cover Page above. By signing this Cover Page, each party agrees to enter into this Agreement as of the Effective Date.

	PROVIDER: eesel, Inc	**CUSTOMER:**
Signature		
Print Name		
Title		
Notice Address	651 N Broad St Middletown, Delaware 19709 United States of America	
Date		

Data Processing Agreement

1. Processor and Subprocessor Relationships

1.1. Provider as Processor. In situations where Customer is a Controller of the Customer Personal Data, Provider will be deemed a Processor that is Processing Personal Data on behalf of Customer .

1.2. Provider as Subprocessor. In situations where Customer is a Processor of the Customer Personal Data, Provider will be deemed a Subprocessor of the Customer Personal Data.

2. Processing

2.1. Processing Details. Annex I(B) on the Cover Page describes the subject matter, nature, purpose, and duration of this Processing, as well as the Categories of Personal Data collected and Categories of Data Subjects .

2.2. Processing Instructions. Customer instructs Provider to Process Customer Personal Data: (a) to provide and maintain the Service; (b) as may be further specified through Customer's use of the Service; (c) as documented in the Agreement ; and (d) as documented in any other written instructions given by Customer and acknowledged by Provider about Processing Customer Personal Data under this DPA. Provider will abide by these instructions unless prohibited from doing so by Applicable Laws. Provider will immediately inform Customer if it is unable to follow the Processing instructions. Customer has given and will only give instructions that comply with Applicable Laws.

2.3. Processing by Provider. Provider will only Process Customer Personal Data in accordance with this DPA, including the details in the Cover Page. If Provider updates the Service to update existing or include new products, features, or functionality, Provider may change the Categories of Data Subjects , Categories of Personal Data , Special Category Data , Special Category Data Restrictions or Safeguards , Frequency of Transfer , Nature and Purpose of Processing , and Duration of Processing as needed to reflect the updates by notifying Customer of the updates and changes.

2.4. Customer Processing. Where Customer is a Processor and Provider is a Subprocessor, Customer will comply with all Applicable Laws that apply to Customer's Processing of Customer Personal Data. Customer's agreement with its Controller will similarly require Customer to comply with all Applicable Laws that apply to Customer as a Processor. In addition, Customer will comply with the Subprocessor requirements in Customer's agreement with its Controller.

2.5. Consent to Processing. Customer has complied with and will continue to comply with all Applicable Data Protection Laws concerning its provision of Customer Personal Data to Provider and/or the Service, including making all disclosures, obtaining all consents, providing adequate choice, and implementing relevant safeguards required under Applicable Data Protection Laws.

2.6. Subprocessors.

a. Provider will not provide, transfer, or hand over any Customer Personal Data to a Subprocessor unless Customer has approved the Subprocessor. The current list of Approved Subprocessors includes the identities of the Subprocessors, their country of location, and their anticipated Processing tasks. Provider will inform Customer at least 10 business days in advance and in writing of any intended changes to the Approved Subprocessors whether by addition or replacement of a Subprocessor, which allows Customer to have enough time to object to the changes before the Provider begins using the new Subprocessor(s). Provider will give Customer the information necessary to allow Customer to exercise its right to object to the change to Approved Subprocessors . Customer has 30 days after notice of a change to the Approved Subprocessors to object, otherwise Customer will be deemed to accept the changes. If Customer objects to the change within 30 days of notice, Customer and Provider will cooperate in good faith to resolve Customer's objection or concern.

b. When engaging a Subprocessor, Provider will have a written agreement with the Subprocessor that ensures the Subprocessor only accesses and uses Customer Personal Data (i) to the extent required to perform the obligations subcontracted to it, and (ii) consistent with the terms of Agreement .

c. If the GDPR applies to the Processing of Customer Personal Data, (i) the data protection obligations described in this DPA (as referred to in Article 28(3) of the GDPR, if applicable) are also imposed on the Subprocessor, and (ii) Provider's agreement with the Subprocessor will incorporate these obligations, including details about how Provider and its Subprocessor will coordinate to respond to inquiries or requests about the Processing of Customer Personal Data. In addition, Provider will share, at Customer's request, a copy of its agreements (including any amendments) with its Subprocessors. To the extent necessary to protect business secrets or other confidential information, including personal data, Provider may redact the text of its agreement with its Subprocessor prior to sharing a copy.

d. Provider remains fully liable for all obligations subcontracted to its Subprocessors, including the acts and omissions of its Subprocessors in Processing Customer Personal Data. Provider will notify Customer of any failure by its Subprocessors to fulfill a material obligation about Customer Personal Data under the agreement between Provider and the Subprocessor.

3. Restricted Transfers

3.1. Authorization. Customer agrees that Provider may transfer Customer Personal Data outside the EEA, the United Kingdom, or other relevant geographic territory as necessary to provide the Service. If Provider transfers Customer Personal Data to a territory for which the European Commission or other relevant supervisory authority has not issued an adequacy decision, Provider will implement appropriate safeguards for the transfer of Customer Personal Data to that territory consistent with Applicable Data Protection Laws.

3.2. Ex-EEA Transfers. Customer and Provider agree that if the GDPR protects the transfer of Customer Personal Data, the transfer is from Customer from within the EEA to Provider outside of the EEA, and the transfer is not governed by an adequacy decision made by the European Commission, then by entering into this DPA, Customer and Provider are deemed to have signed the EEA SCCs and their Annexes, which are incorporated by reference. Any such transfer is made pursuant to the EEA SCCs, which are completed as follows:

a. Module Two (Controller to Processor) of the EEA SCCs apply when Customer is a Controller and Provider is Processing Customer Personal Data for

Customer as a Processor.

b. Module Three (Processor to Sub-Processor) of the EEA SCCs apply when Customer is a Processor and Provider is Processing Customer Personal Data on behalf of Customer as a Subprocessor.

c. For each module, the following applies (when applicable):

i. The optional docking clause in Clause 7 does not apply;

ii. In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of Subprocessor changes is 10 business days;

iii. In Clause 11, the optional language does not apply;

iv. All square brackets in Clause 13 are removed;

v. In Clause 17 (Option 1), the EEA SCCs will be governed by the laws of Governing Member State ;

vi. In Clause 18(b), disputes will be resolved in the courts of the Governing Member State ; and

vii. The Cover Page to this DPA contains the information required in Annex I, Annex II, and Annex III of the EEA SCCs.

3.3. Ex-UK Transfers. Customer and Provider agree that if the UK GDPR protects the transfer of Customer Personal Data, the transfer is from Customer from within the United Kingdom to Provider outside of the United Kingdom, and the transfer is not governed by an adequacy decision made by the United Kingdom Secretary of State, then by entering into this DPA, Customer and Provider are deemed to have signed the UK Addendum and their Annexes, which are incorporated by reference. Any such transfer is made pursuant to the UK Addendum, which is completed as follows:

a. Section 3.2 of this DPA contains the information required in Table 2 of the UK Addendum.

b. Table 4 of the UK Addendum is modified as follows: Neither party may end the UK Addendum as set out in Section 19 of the UK Addendum; to the extent ICO issues a revised Approved Addendum under Section 18 of the UK Addendum, the parties will work in good faith to revise this DPA accordingly.

c. The Cover Page contains the information required by Annex 1A, Annex 1B, Annex II, and Annex III of the UK Addendum.

3.4. Other International Transfers. For Personal Data transfers where Swiss law (and not the law in any EEA member state or the United Kingdom) applies to the international nature of the transfer, references to the GDPR in Clause 4 of the EEA SCCs are, to the extent legally required, amended to refer to the Swiss Federal Data Protection Act or its successor instead, and the concept of supervisory authority will include the Swiss Federal Data Protection and Information Commissioner.

4. Security Incident Response

4.1. Upon becoming aware of any Security Incident, Provider will: (a) notify Customer without undue delay when feasible, but no later than 72 hours after becoming aware of the Security Incident; (b) provide timely information about the Security Incident as it becomes known or as is reasonably requested by Customer ; and (c) promptly take reasonable steps to contain and investigate the Security Incident. Provider's notification of or response to a Security Incident as required by this DPA will not be construed as an acknowledgment by Provider of any fault or liability for the Security Incident.

5. Audit & Reports

5.1. Audit Rights. Provider will give Customer all information reasonably necessary to demonstrate its compliance with this DPA and Provider will allow for and contribute to audits, including inspections by Customer , to assess Provider's compliance with this DPA. However, Provider may restrict access to data or information if Customer's access to the information would negatively impact Provider's intellectual property rights, confidentiality obligations, or other obligations under Applicable Laws. Customer acknowledges and agrees that it will only exercise its audit rights under this DPA and any audit rights granted by Applicable Data Protection Laws by instructing Provider to comply with the reporting and due diligence requirements below. Provider will maintain records of its compliance with this DPA for 3 years after the DPA ends.

5.2. Security Reports. Customer acknowledges that Provider is regularly audited against the standards defined in the Security Policy by independent third-party auditors. Upon written request, Provider will give Customer , on a confidential basis, a summary copy of its then-current Report so that Customer can verify Provider's compliance with the standards defined in the Security Policy .

5.3. Security Due Diligence. In addition to the Report, Provider will respond to reasonable requests for information made by Customer to confirm Provider's compliance with this DPA, including responses to information security, due diligence, and audit questionnaires, or by giving additional information about its information security program. All such requests must be in writing and made to the Provider Security Contact and may only be made once a year.

6. Coordination & Cooperation

6.1. Response to Inquiries. If Provider receives any inquiry or request from anyone else about the Processing of Customer Personal Data, Provider will notify Customer about the request and Provider will not respond to the request without Customer's prior consent. Examples of these kinds of inquiries and requests include a judicial or administrative or regulatory agency order about Customer Personal Data where notifying Customer is not prohibited by Applicable Law, or a request from a data subject. If allowed by Applicable Law, Provider will follow Customer's reasonable instructions about these requests, including providing status updates and other information reasonably requested by Customer . If a data subject makes a valid request under Applicable Data Protection Laws to delete or opt out of Customer's giving of Customer Personal Data to Provider , Provider will assist Customer in fulfilling the request according to the Applicable Data Protection Law. Provider will cooperate with and provide reasonable assistance to Customer , at Customer's expense, in any legal response or other procedural action taken by Customer in response to a third-party request about Provider's Processing of Customer Personal Data under this DPA.

6.2. DPIAs and DTIAs. If required by Applicable Data Protection Laws, Provider will reasonably assist Customer in conducting any mandated data protection impact assessments or data transfer impact assessments and consultations with relevant data protection authorities, taking into consideration the nature of the Processing and Customer Personal Data.

7. Deletion of Customer Personal Data

7.1. Deletion by Customer. Provider will enable Customer to delete Customer Personal Data in a manner consistent with the functionality of the Services. Provider will comply with this instruction as soon as reasonably practicable except where further storage of Customer Personal Data is required by Applicable Law.

7.2. Deletion at DPA Expiration.

a. After the DPA expires, Provider will return or delete Customer Personal Data at Customer's instruction unless further storage of Customer Personal Data is required or authorized by Applicable Law. If return or destruction is impracticable or prohibited by Applicable Laws, Provider will make reasonable efforts to prevent additional Processing of Customer Personal Data and will continue to protect the Customer Personal Data remaining in its possession, custody, or control. For example, Applicable Laws may require Provider to continue hosting or Processing Customer Personal Data.

b. If Customer and Provider have entered the EEA SCCs or the UK Addendum as part of this DPA, Provider will only give Customer the certification of deletion of Personal Data described in Clause 8.1(d) and Clause 8.5 of the EEA SCCs if Customer asks for one.

8. Limitation of Liability

8.1. Liability Caps and Damages Waiver. **To the maximum extent permitted under Applicable Data Protection Laws, each party's total cumulative liability to the other party arising out of or related to this DPA will be subject to the waivers, exclusions, and limitations of liability stated in the Agreement .**

8.2. Related-Party Claims. **Any claims made against Provider or its Affiliates arising out of or related to this DPA may only be brought by the Customer entity that is a party to the Agreement .**

8.3. Exceptions. This DPA does not limit any liability to an individual about the individual's data protection rights under Applicable Data Protection Laws. In addition, this DPA does not limit any liability between the parties for violations of the EEA SCCs or UK Addendum.

9. Conflicts Between Documents

9.1. This DPA forms part of and supplements the Agreement. If there is any inconsistency between this DPA, the Agreement , or any of their parts, the part listed earlier will control over the part listed later for that inconsistency: (1) the EEA SCCs or the UK Addendum, (2) this DPA, and then (3) the Agreement .

10. Term of Agreement

10.1. This DPA will start when Provider and Customer agree to a Cover Page for the DPA and sign or electronically accept the Agreement and will continue until the Agreement expires or is terminated. However, Provider and Customer will each remain subject to the obligations in this DPA and Applicable Data Protection Laws until Customer stops transferring Customer Personal Data to Provider and Provider stops Processing Customer Personal Data.

11. Definitions

11.1. **"Applicable Laws"** means the laws, rules, regulations, court orders, and other binding requirements of a relevant government authority that apply to or govern a party.

11.2. **"Applicable Data Protection Laws"** means the Applicable Laws that govern how the Service may process or use an individual's personal information, personal data, personally identifiable information, or other similar term.

11.3. **"Controller"** will have the meaning(s) given in the Applicable Data Protection Laws for the company that determines the purpose and extent of Processing Personal Data.

11.4. **"Cover Page"** means a document that is signed or electronically accepted by the parties that incorporates these DPA Standard Terms and identifies Provider , Customer , and the subject matter and details of the data processing.

11.5. **"Customer Personal Data"** means Personal Data that Customer uploads or provides to Provider as part of the Service and that is governed by this DPA.

11.6. **"DPA"** means these DPA Standard Terms, the Cover Page between Provider and Customer , and the policies and documents referenced in or attached to the Cover Page.

11.7. **"EEA SCCs"** means the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the European Council.

11.8. **"European Economic Area"** or **"EEA"** means the member states of the European Union, Norway, Iceland, and Liechtenstein.

11.9. **"GDPR"** means European Union Regulation 2016/679 as implemented by local law in the relevant EEA member nation.

11.10. **"Personal Data"** will have the meaning(s) given in the Applicable Data Protection Laws for personal information, personal data, or other similar term.

11.11. **"Processing"** or **"Process"** will have the meaning(s) given in the Applicable Data Protection Laws for any use of, or performance of a computer operation on, Personal Data, including by automatic methods.

11.12. **"Processor"** will have the meaning(s) given in the Applicable Data Protection Laws for the company that Processes Personal Data on behalf of the Controller.

11.13. **"Report"** means audit reports prepared by another company according to the standards defined in the Security Policy on behalf of Provider.

11.14. **"Restricted Transfer"** means (a) where the GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; and (b) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not subject to adequacy regulations adopted pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

11.15. **“Security Incident”** means a Personal Data Breach as defined in Article 4 of the GDPR.

11.16. **“Service”** means the product and/or services described in the **Agreement** .

11.17. **“Special Category Data”** will have the meaning given in Article 9 of the GDPR.

11.18. **“Subprocessor”** will have the meaning(s) given in the Applicable Data Protection Laws for a company that, with the approval and acceptance of Controller, assists the Processor in Processing Personal Data on behalf of the Controller.

11.19. **“UK GDPR”** means European Union Regulation 2016/679 as implemented by section 3 of the United Kingdom’s European Union (Withdrawal) Act of 2018 in the United Kingdom.

11.20. **“UK Addendum”** means the international data transfer addendum to the EEA SCCs issued by the Information Commissioner for Parties making Restricted Transfers under S119A(1) Data Protection Act 2018.

EXHIBIT A

SECURITY MEASURES

For the purpose of this supplemental document, the term "Service Provider," also referred to as "Provider," shall consistently denote "eesel, Inc." in alignment with the terminology used in the Cloud Services Agreement. In instances where eesel, Inc. offers Software as a Service (SaaS) solutions, it explicitly affirms and guarantees to the Company that:

1. INFORMATION SECURITY MANAGEMENT SYSTEM

1.1. Information security is managed through a stringent set of controls, including policies, processes, procedures, software, and hardware functions that constitute Service Provider’s Information Security Management System (“**ISMS**”). These controls are monitored, reviewed, and, where necessary, improved to ensure that specific security and business objectives are met.

1.2. All employees receive a comprehensive and mandatory induction and training program on joining the company and an annual compliance refresher including information security and data protection.

1.3. The Service Provider shall appoint dedicated personnel to manage information security and data protection (DPO) and shall be ultimately responsible for risk and security incident management and shall act as the central point of contact for information security for both employees and external organizations.

2. HUMAN RESOURCE SECURITY

2.1. Service Provider ensures that pre-employment screening requirements are carried out according to applicable local laws.

2.2. Confidentiality clauses are in place in employees’ contracts and third-party vendors that provide adequate protection for the confidentiality of Service Provider Data.

2.3. A disciplinary process is in place to address non-compliance with security policies and requirements.

2.4. Upon termination of employment, access is revoked from employees on their last working day and all equipment and proprietary information is returned by the leaver.

2.5. The Service Provider shall notify the Company immediately and with undue delay about terminated employees with direct Company’s systems access or holding Company’s credentials.

3. ASSET MANAGEMENT AND DATA SECURITY

3.1. Assets associated with information and information-processing facilities shall be identified and an inventory of assets is maintained.

3.2. Information and Data shall be classified and managed in line with a management approved Information Classification & Data Management Policy.

3.3. Only trusted devices shall have access to Service Provider corporate network resources. These include Service Provider computers and mobile devices.

3.5. A Data Retention Policy and Data Retention Schedule are in place to define data retention requirements in line with GDPR and the Data Protection Act, as well as secure data disposal requirements of sensitive data on physical or electronic media to recognized IT industry security standards / best practices.

3.6. Customer Data shall be stored in a SOC2 type II certified data center.

3.7. Media containing any information shall be destroyed using secure means of disposal in accordance with NIST or similar data destruction standards.

3.8. Service Provider shall put in place controls to restrict employees' access to Customer Data and storage of scoped systems.

3.9. Service Provider shall assure Company's data is segregated using unique identifiers assigned at the time of account implementation and proper data isolation shall exist on multi-tenant environments.

4. ACCESS CONTROL

4.1. Service Provider shall utilize a Role Based Access Control model with roles assigned to individuals based on job roles and need-to-know basis.

4.2. Service Provider shall apply separation of Duties and Least privilege Principles and shall manage privileged access upon documented approval process by senior management.

4.3. Service Provider shall assure privileged IT administrative rights are provided via a separate User ID (elevated account) to the user's normal User ID.

4.4. Service Provider shall monitor all events associated with log in to servers with administrative accounts and as well changes/modifications to privilege groups.

4.5. Service Provider shall assure access rights reviews are conducted periodically with the frequency depending on the criticality of the information asset and varying between quarterly to annually.

4.6. The Service Provider shall maintain a strong password policy throughout all their systems.

4.7. Multifactor authentication is enforced on all Service Provider users and administrative accounts.

4.8. Where possible, Service Provider enforces SSO with an identity provider.

5. CRYPTOGRAPHY

5.1. Service Provider shall implement cryptographic controls to protect sensitive data both whilst in transit and at rest.

5.2. Database encryption shall be in place via AES 256-Bit Encryption or higher, data tokenization.

5.3. All traffic from/to Public facing applications (public websites + SaaS platform) shall utilize HTTPS certificates encrypted with TLS 1.2 or higher.

5.4. Service Provider shall encrypt and apply authentication to all public API endpoints and buckets.

5.5. All backups shall be encrypted at rest.

6. OPERATIONS SECURITY

6.1. Service Provider changes to production environments shall be controlled, approved by relevant owners, and documented.

6.2. Service Provider shall apply malware detection, prevention, and recovery controls and next generation anti-malware solution in all the endpoints and servers.

6.3. Service Provider shall apply a comprehensive patch management process. Patches and security updates shall be deployed monthly, or more frequently if a significant security risk is identified. Service Provider shall maintain a technical vulnerability management program including an ongoing program of remediation. Vulnerabilities shall be identified via internal and external infrastructure scans, SAC/DAST scans, and configuration tests.

6.4. Service Provider shall perform a comprehensive annual penetration test program, carried out by accredited independent penetration testers.

7. LOGGING, MONITORING & SECURITY INCIDENT MANAGEMENT

7.1. Service Provider shall manage event logging, recording user activities, exceptions, faults, and audit trails. Information security events shall be generated, reviewed, retained for at least 1 year, and protected from tampering.

7.2. Service Provider shall analyze security information events, and shall perform security incident response & mitigation, including a proper RCA to understand the cause of security incidents and methods of reducing or removing potential areas for attack.

7.3. Service Provider shall notify the Company about security breach without undue delay, and no longer than 48 hours.

8. COMMUNICATION & NETWORK SECURITY

8.1. Service Provider's network shall be managed through appropriate security controls such as network segmentation, network access management, firewalls, configuration standards, and logging and monitoring.

8.2. Service Provider's assets shall be segregated via dedicated VPCs and Security Groups. Proper Prod, Dev, staging, and other test environments shall be configured to make sure each environment is destined for the mentioned purposes.

8.3. Service Provider shall implement WAF and DDoS protections on the production environment where Company's data and tenant resides.

9. PHYSICAL SECURITY

9.1. Service Provider shall maintain adequate physical and environmental security measures to prevent unauthorized physical access, damage, and interference to Service Provider's data, premises, and processing facilities. The minimum controls as the following:

9.1.1. Offices:

9.1.1.1. Manned building reception operating during office hours. CCTV at all building access points provides coverage of the most common areas and the areas of ingress and egress from the building. Entry is restricted to authorized individuals with a business need.

9.1.1.2. Visitors shall be granted access for specific and authorized purposes only and are always supervised/escorted whilst in the Cloud Provider's offices. Visitor logs shall be maintained for all physical access to offices, server rooms, and data centers hosting Service Provider's information assets.

10. SOFTWARE DEVELOPMENT

10.1. Service Provider shall implement a S-SDLC (Secure Software Development Lifecycle) Policy including requirements analysis and specifications, security by design, secure engineering principles, secure development environment, application support, QA, testing, implementation, training, and post-implementation review.

10.2. Service Provider shall follow secure development best practices such as OWASP, NIST, or similar.

10.3. Service Provider shall procure that an ongoing code review is conducted according to best practices and with proper tools, including SAST, DAST, and other methodologies, covering open source, IaC, and others.

11. SUPPLIER RELATIONSHIPS

11.1. Service Provider shall assure that every direct supplier (including data sub-processors) undergoes due diligence covering Information Security, Data Protection, Business Continuity, policies review, annually reviewed and approved certifications, independent audit reports, and independent penetration tests.

11.2. Service Provider shall assure suppliers are subject to confidentiality, security, and right to audit clauses within their contracts.

11.3. Service Provider shall assure suppliers are reviewed on a periodic basis. The nature, scope, and frequency of this review depends on several factors including the product/service being provided and the supplier's criticality.

11.4. Service Provider shall notify with undue delay the change on any sub-processor, giving the Company the right to reject the adoption and data transfer of the same.

12. BUSINESS CONTINUITY AND DISASTER RECOVERY

12.1. Service Provider shall assure business continuity plans are formally reviewed and exercised on an annual basis, or more frequently if necessary (e.g., if there is a significant change).

12.2. Service Provider shall assure an annual Business Impact Analysis is carried out to define the amount of disruption the business can tolerate to its key activities; the minimum level of these activities required for operation; and the resources and dependencies required to resume activities.

12.3. Service Provider shall perform backups to ensure that critical information contained within storage and databases is stored securely and independently and is available for restoration in the event of accidental loss or corruption.

12.4. Service Provider shall maintain a minimum RTO of 4hs and RPO of 24hs.

12.5. Backups shall be tested periodically.

13. INFORMATION SECURITY RISK

13.1. The Service Provider shall perform a security risk management program that covers the identification and assessment of Information Security risks arising both from various periodic activities and from planned and unplanned change. Identified risks shall be prioritized, treated/accepted, and approved in a timely manner.

If the Service Provider provides Consulting services, it hereby represents and warrants to the Company that:

1. Introduction:

1. This Security Measures Document outlines the information security practices that service providers and consultants shall adhere to during the course of their engagement with the Company. These measures are designed to protect Company's sensitive data, systems, and infrastructure, and ensure compliance with industry best practices. By following these guidelines, we can maintain a secure environment and mitigate potential risks.

2. Access Control:

   o Service Provider shall adhere to the principle of least privilege, granting access only to the resources necessary for its assigned tasks.

   o Strong and unique passwords must be used for all accounts, including system logins, email, and any other relevant platforms.

   o Two-factor authentication (2FA) should be enabled wherever possible to enhance account security.

   o To the extent applicable, Service Provider will access Company's systems according to defined processes, tools and methods for service providers and consultants as explained and designed by the Company's IT and Security teams.

3. Data Protection:

   o Confidential and sensitive data must be handled with utmost care and only shared with authorized personnel on a need-to-know basis.

   o Service Provider shall not store company data on personal devices or cloud services without explicit permission.

   o Encryption should be used when transmitting or storing sensitive information to protect it from unauthorized access.

4. Physical Security:

   o Service Provider shall maintain the physical security of its work area, ensuring that unauthorized individuals cannot access its premises or working area where sensitive materials are exposed.

   o Laptops, mobile devices, and other portable storage media should be protected with strong passwords or biometric authentication.

5. Software and System Security:

   o Service Provider shall keep their work devices and software up to date with the latest security patches and updates.

   o Only approved software and applications should be installed on smart devices.

   o Antivirus and anti-malware software must be installed and regularly updated to prevent and detect any potential threats.

6. Network Security:

- Service Provider shall only connect to secure and trusted networks, avoiding public Wi-Fi or unsecured networks whenever possible.
- VPN (Virtual Private Network) connections should be used when accessing company resources remotely to ensure secure communication.
- Regular network scans and vulnerability assessments should be conducted to identify and mitigate potential security weaknesses.

7. Incident Reporting:

- Service Provider shall report any security incidents, breaches, or suspected vulnerabilities immediately to the designated contact person at Company's Infosec department. Incidents will include the loss of personal or work devices which the Service Provider used to work on Company's projects or handle Company's Proprietary Information.
- Cooperation and support should be provided during incident response procedures to minimize the impact of any security events.

8. Confidentiality and Non-Disclosure:

- Service Provider shall comply with all of its confidentiality and non-disclosure obligations to safeguard the Company's information.
- Proprietary information, trade secrets, and client data must be treated with the utmost confidentiality and should not be shared externally without proper authorization.