Sembi Affiliates Data Processing Terms
(for the Customer-Facing DPA)

Details of Processing of Kiuwan Software, S.L.

a. **Address: –**
   Calle de Velázquez, nº 157 - 1ª Plta, 28002 - Madrid Spain
b. **Type of Services provided by the Sembi Affiliate involving the Processing of Customer Personal Data: –**
    i. Kiuwan provides an end-to-end application security platform to bring objective data and facilitate informed decisions regarding the cost, effort, activity, quality, maintainability, efficiency, and dependencies of the company's applications.
c. **Data Protection Officer (DPO) Details: –**
   VeraSafe, LLC, a Delaware limited liability company.
   experts@verasafe.com
d. **EU Data Protection Representative: –**
   n/a
e. **UK Data Protection Representative: –**
   VeraSafe United Kingdom Ltd.
   37 Albert Embankment London SE1 7TL United Kingdom
   Contact form:
   https://verasafe.com/public-resources/contact-data-protection-representative
f. **Subject matter and duration: –**
   The subject matter and duration of the Processing of Customer Personal Data are set forth in the Main Agreement and all amendments, exhibits, schedules, task orders, addenda, SOWs, purchase orders and other documents associated therewith and incorporated therein.
g. **Nature and Purpose of Processing: –**
   The nature and purpose of the Processing of Customer Personal Data are set forth in the Main Agreement and all amendments, exhibits, schedules, task orders, addenda, SOWs, purchase orders and other documents associated therewith and incorporated therein.

h. **Further Processing: –**
   No further Processing of Customer Personal Data beyond the Processing necessary for the provision of the Services is allowed.
i. **Categories of Data Subjects: –**
   Data subjects may include Customer's representatives, such as employees, contractors, collaborators, partners. Data subject may also include individuals attempting to communicate or transfer Customer Personal Data to users of the Services.
j. **Categories of Customer Personal Data: –**
   The Categories of Customer Personal Data that Customer authorizes and requests that Kiuwan Processes include but are not limited to: Professional contact data of customer employees, temporary staff, trainees, apprentices (professional telephone number/email address, department affiliation).
k. **Special Categories of Customer Personal Data to be Processed (if applicable) and the applied restrictions to the Processing of these Special Categories of Customer Personal Data: –**
   n/a
l. **Categories of third-party recipients to whom the Customer Personal Data may be disclosed or shared by Kiuwan: –**
   Subprocessors; and other Sembi Affiliates, if applicable.
m. **Frequency of the Transfer of Customer Personal Data: –**
   The frequency of the transfer of Customer Personal Data is determined by the Customer. Customer Personal Data is transferred each time that the Customer instructs Kiuwan to Process Customer Personal Data.
n. **Maximum data retention periods, if applicable: –**
   The retention period of the Customer Personal Data is generally determined by the Customer and is subject to the term of the DPA and the Main Agreement, respectively, in the context of the contractual relationship between Kiuwan and the Customer.
o. **The basic Processing activities to which Customer Personal Data will be subject include, without limitation: –**
   Collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction for the purpose of providing the Services to Customer in accordance with the terms of the Main Agreement.

p. **The following is deemed an instruction by the Customer to Kiuwan to Process Customer Personal Data: –**
    i. Processing in accordance with the Main Agreement.
    ii. Processing initiated by Data Subjects in their use of the Services.
    iii. Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Main Agreement.

q. **List of Kiuwan's Subprocessors available at** https://www.ideracorp.com/Legal/Kiuwan/Subprocessors

r. **Description of technical and organizational security measures implemented by the Kiuwan: –**
    i. Measures of pseudonymization and encryption of Customer Personal Data:
        a. Encryption of the transferred Customer Personal Data in transit using the Transport Layer Security (TLS) protocol version 1.2 or higher with a minimum of 128-bit encryption;
        b. Encryption at rest within Kiuwan's software applications using a minimum of AES-256.
    ii. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services:
        a. Restriction of logical access to IT systems that Process transferred Customer Personal Data to those officially authorized persons with an identified need for such access;
        b. Active monitoring and logging of network and database activity for potential security events, including intrusion;
        c. Regular scanning and monitoring of any unauthorized software applications and IT systems for vulnerabilities of Kiuwan;
        d. Firewall protection of external points of connectivity in Data Importer's network architecture; and
        e. Expedited patching of known exploitable vulnerabilities in the software applications and IT systems used by Kiuwan.
        f. Key management/documentation of key issuance.
        g. Security Zones Concept
        h. Physical access control system, e.g. badge reader (magnetic/chip cards).

i. Factory security / gatekeeper
j. Security doors / security windows
k. Door protection (electrical door opener, combination lock, etc.)
l. Alarm system
m. Video surveillance
n. Special server room protection measures
o. Locked filing cabinets
p. Guideline for a tidy working environment

iii. Measures for ensuring the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident:
a. Backup procedures.
b. Secured storage of backups.

iv. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the Processing
a. Management process for security incidents;
b. Management process for incidents relevant to data protection;
c. Definition of security requirements in crisis situations / emergencies;
d. Comprehensive emergency plan incl. regular updating; and
e. Regular execution and documentation of emergency tests.

v. Measures for user identification and authorization:
a. Appropriate authorization concepts:
i. Responsibilities;
ii. Task-related profiles and roles; and
iii. Target role concept.
b. User management process incl. approval procedure;

vi. Measures for the protection of data during transmission:
a. Encryption of the transferred Customer Personal Data in transit using the Transport Layer Security (TLS) protocol version 1.2 or higher with a minimum of 128-bit encryption;
b. Tunnelled remote data transfer connections (VPN = Virtual Private Network);

c. SSL/TLS encryption;

vii. Measures for the protection of data during storage:
    a. Data is stored using a leading service that ensures high performance, scalability, availability and security by default; and
    b. Access is role based and reviewed regularly.

viii. Measures for ensuring physical security of locations at which Customer Personal Data are processed:
    a. Restriction of physical to IT systems that Process transferred Customer Personal Data to those officially authorized persons with an identified need for such access;
    b. Users have a unique personal identifier;
    c. Separate user IDs for privileged authorizations;
    d. Passwords are generally not stored in plain text or transmitted unencrypted;
    e. Secure password procedures;
    f. Secure generation and transmission of initial and reset passwords;
    g. Automatic locking of the clients after time lapse without user activity (e.g. password-protected screen saver);
    h. Continuous software updates / patching (patch Management);
    i. Continuous vulnerability scans;
    j. Firewall, IDS/IPS; and
    k. Monitoring of remote maintenance access by service providers.

ix. Measures for ensuring events logging:
    a. Active monitoring and logging of network and database activity for potential security events, including intrusion.
    b. Usage of security/logging software;
    c. Processing of data in accordance with applicable legal requirements for information security;
    d. Logs are protected against unauthorized access (confidentiality);
    e. Logs are protected against unauthorized modification (integrity); and

f. Logs are protected against loss (availability).

x. Measures for ensuring system configuration, including default configuration:
    a. Applications use standard configurations and they are scanned against best practices and vulnerabilities.

xi. Measures for internal IT and IT security governance and management:
    a. Users are created with only required permissions and access roles;
    b. Permissions are reviewed and removed regularly; and

xii. Measures for certification/assurance of processes and products:
    a. Kiuwan is SOC-2 Type 2 certified.

xiii. Measures for ensuring data minimization:
    a. Data minimization is guaranteed during the design and implementation processes.

xiv. Measures for ensuring data quality:
    a. Customer is responsible for data quality and accuracy since the data is provided by the Customer; and
    b. Form validations are made to validate some fields.

xv. Measures for ensuring limited data retention:
    a. Different policies can apply depending on the type of data.

xvi. Measures for ensuring accountability:
    a. Documentation about how personal data is processed.

xvii. Measures for allowing data portability and ensuring erasure:
    a. In-product feature to allow data portability that securely transmits the data structured in a readable format; and
    b. A formal Compliance process for deleting Customer Personal Data by making a support request.

xviii. Other:
    a. Internal policies establishing that
        a. Where Kiuwan is prohibited by law from notifying Data Exporter of an order from a public authority for transferred Customer Personal Data, Kiuwan shall take into account the laws of other jurisdictions and use best efforts to request that any confidentiality requirements be waived to

enable it to notify the competent Supervisory Authorities;

b. Kiuwan must require an official, signed document issued pursuant to the applicable laws of the requesting third party before it will consider a request for access to transferred Customer Personal Data;
c. Kiuwan shall scrutinize every request for legal validity and, as part of that procedure, will reject any request Data Importer considers to be invalid; and
d. If Kiuwan is legally required to comply with an order, it will respond as narrowly as possible to the specific request.