JOSYS DATA PROCESSING ADDENDUM

Revised: April 22, 2026

This Data Processing Addendum ("**DPA**") forms a part of the Josys Services Agreement or the Josys Professional Services Terms and Conditions, each as applicable, (the "**Agreement**") between Josys and the Customer and reflects the Parties' agreement with regard to the processing of Customer Personal Data. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In providing the Services to Customer pursuant to the Agreement, Josys may process Customer Personal Data on behalf of the Customer and the Parties agree to comply with the following provisions with respect to any Customer Personal Data. For clarity, at its sole discretion, Josys may amend this DPA, but any such amendment(s) shall not materially increase Customer's liabilities or obligations, nor shall it materially decrease Josys' obligations or liabilities unless required by Data Protection Laws (as defined below).

1. Definitions.

"Data Protection Laws" means all laws and regulations applicable to the Processing of Customer Personal Data under the Agreement including, without limitation: (a) the Japan Act concerning the Protection of Personal Information as amended and any binding regulations promulgated thereunder ("APPI"), (b) the California Consumer Privacy Act as amended by the California Privacy Rights Act and any binding regulations promulgated thereunder ("CCPA"), (c) General Data Protection Regulation (EU 2016/679) ("EU GDPR"), (d) the UK Data Protection Act 2018 ("UK GDPR), and (e) the Australia Privacy Act 1988 (Cth), in each case, as updated, amended or replaced from time to time.

"***Data Subject***" means an identified or identifiable natural person, or such other similar term as may be defined by applicable Data Protection Laws.

"**Personal Data**" means any information relating to an identified or identifiable natural person as defined under Data Protection Laws that Customer and its Tenants provides or makes available to Josys as part of the Services.

"**Process**", "**Processing**", "**Processor**", "**Controller**", and "**Data Subject**" have the meanings set forth in the EU GDPR.

"***Restricted Transfer***" means: (a) where the APPI applies, a transfer of Personal Data to a country outside Japan that is not recognized by the Personal Information Protection Commission to have equivalent standards to that in Japan, (b) where the EU GDPR applies, a transfer of Personal Data to a country outside the EEA that is not subject to an adequacy determination, (c) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country that is not subject to an adequacy determination, and (d) with respect to any other country where the applicable Data Protection Laws restrict international transfers, an international transfer to a country that is not subject to an adequacy decision or otherwise requires some form of transfer mechanism to be implemented in order to comply with applicable Data Protection Laws (hereinafter referred to as, "***Other Restricted***

***Transfer**").*

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data while being processed by Josys. Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

"**Standard Contractual Clauses**" means, as applicable, (i) with respect to restricted transfers subject to EU GDPR, the Controller-to-Processor standard contractual clauses or the Processor-to-Processor standard clauses (as applicable) adopted by the European Commission pursuant to its Implementing Decision (EU) 2021/914 of 4 June 2021, on standard clauses for the transfer of personal data to third countries pursuant to the EU GDPR, as may be amended or replaced by the European Commission from time to time (the "***EU SCCs***") , (ii) with respect to restricted transfers subject to the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, as may be amended or replaced by the UK Information Commissioner's Office from time to time (the "***UK SCCs***"), and (iii) with respect to Other Restricted Transfers subject to other applicable Data Protection Laws, such other standard contract clauses or transfer mechanisms that is required to be implemented between Josys and Customer ("***Other Applicable Transfer Clauses***").

"***Subprocessor***" means any third party or Josys Affiliate engaged by Josys to Process Personal Data on behalf of Josys.

2. Processing of Personal Data.

2.1. This DPA applies when Personal Data is Processed by Josys on behalf of Customer. As between Customer and Josys, at all times Customer will act as the "Controller" and Josys will act as the "Processor" with respect to the Personal Data.

2.2. The subject matter of the Processing under this DPA is Personal Data provided to Josys by Customer and its Tenants in connection with the Services. The duration of the Processing under this DPA is for the term of this DPA and the Agreement. The purpose of the Processing of Personal Data under this DPA is for Josys to provide the Services to Customer. The nature of the Processing is the provision of the Services by Josys and as more specifically described in the Agreement. The type of data is the Personal Data uploaded to the Services by Customer and its Tenants at its sole discretion. The categories of Data Subjects may include, but is not limited to employees, contractors, agents, advisors and agents (who are natural persons) of Customer, Tenant and its service providers.

2.3. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of applicable Data Protection Laws, including any applicable requirement to provide notice to, or obtain the consent of, Data Subjects of the use of Josys as Processor.

Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

2.4. Josys shall Process Personal Data received from Customer as a Processor only for the purposes described in the Agreement and as necessary to perform its obligations under the Agreement and strictly in accordance with the documented instructions of Customer except where otherwise required by any applicable Data Protection Laws.

2.5. Josys agrees and certifies that it shall not collect, use, or retain Personal Data except to perform the obligations of the Agreement and will not "sell" or "share" Personal Data (as the terms "sell" and "share" are defined under the CCPA.

3. Restricted Transfers of Personal Data. Josys shall not make international transfers of Personal Data, unless it takes such measures as are necessary to ensure the transfer is in compliance with applicable Data Protection Laws.

3.1. *Japan Transfers*. In the event of a Restricted Transfer of Personal Data from Japan, Josys represents and warrants that it has agreements in place that impose obligations substantially equivalent to the standards required of a Personal Information Handling Business Operator under the APPI **("*Equivalent Measures*")**. Upon 45 days' written notice by Customer and subject to the confidentiality obligations set forth in the Agreement, Josys shall make available to Customer its third party Subprocessors' procedures relevant to the protection of Customer Personal Data in the form of Josys' third-party certifications and audit reports to the extent that its Subprocessors makes them generally available to its customers.

3.2. *EU Transfers*. In the event of a Restricted Transfer of Personal Data from the European Economic Area, the EU SCCs will apply and form part of this DPA. For purposes of the EUSCCs, they will be deemed completed as follows:

a. Where Customer acts as a Controller and Josys acts as a Processor, Module 2 applies.

b. Where Customer acts as a Processor and Josys acts as a Subprocessor, Module 3 applies.

c. Customer is the "data exporter" and Josys is the "data importer";

d. Where applicable the following applies as to the EU SCCs:
   i. the optional docking clause in Clause 7 does not apply;
   ii. in Clause 9, Option 2 will apply, the minimum period for prior notice of a new Subprocessor shall be 30 days, and Josys shall fulfill its notification obligations by notifying Customer of any new Subprocessor in accordance with this DPA;
   iii. in Clause 11, the optional language does not apply;
   iv. in Clause 13, all square brackets are removed with the text meaning;
   v. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;
   vi. in Clause 18(b), disputes will be resolved before the courts of Dublin;
   vii. Annex A of this DPA (Subject Matter and Details of Processing) and/or the order form contains the information required in Annex 1of the EU SCCs, and,

viii. Annex B of this DPA (Technical and Organization Measures) contains the information required in Annex 2 of the EU SCCs.

3.3. *UK Transfers*. In the event of a Restricted Transfer of Personal Data transferred from the United Kingdom, the UK SCCs will apply and form part of this DPA. The UK SCCs will be deemed completed as follows:

a. In Table 1 of the UK SCCs, the parties' key contact information is in Annex A to this DPA and/or the order form;

b. In table 2 of the UK SCCs, the EU SCCs shall apply, including the Appendix Information and with only the following modules, clauses or optional provisions of the EU SCCs brought into effect for the purposes of this DPA:
   i. The applicable Module is Controller to Processor or Processor to Processor, as applicable;
   ii. the optional docking clause in Clause 7 does not apply;
   iii. in Clause 9, Option 2 will apply, the minimum period for prior notice of a new Subprocessor shall be 30 days, and Josys shall fulfill its notification obligations by notifying Customer of any new Subprocessor in accordance with this DPA; and,
   iv. in Clause 11, the optional language does not apply.

c. In Table 3 of the UK SCCs:

   i. the list of parties is in Annex A to this DPA;
   ii. the description of transfer is in Annex A to this DPA;
   iii. Annex II is in Annex B to this DPA; and
   iv. The list of Subprocessors is as set forth in Annex C to this DPA.

d. In Table 4 to the UK SCCs, neither party can terminate the DPA due to a change in law (the respective box is deemed checked).

e. Incorporated herein are Part 2 (Mandatory Clauses) of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

3.4. *Other Restricted Transfer*. In the event of any Other Restricted Transfer, such transfer shall be governed by such Other Applicable Transfer Clauses as may be required under applicable Data Protection Laws, which shall be entered into and incorporated into this DPA by reference and:

a. Annex A and Annex B of this DPA provide details of the Restricted Transfer and Technical and Organizational Measures, respectively; and,

b. Disputes relating to the Other Restricted Transfer shall be governed by the

applicable laws of the country from which the Other Restricted Transfer takes place and resolved before the courts of such country.

4. **Third Party Requests and Confidentiality**. Josys shall not disclose Personal Data to any third party other than: (i) at the request of Customer; (ii) as provided in this DPA; (iii) as necessary to provide the Services; or (iv) as required by applicable law or a valid and binding order of a law enforcement agency. Notwithstanding anything set forth herein, Josys shall ensure that any person that it authorizes to Process the Personal Data shall be subject to a duty of confidentiality and shall not permit any person to Process the Personal Data who is not under such a duty of confidentiality. Except as otherwise required by law, Josys shall promptly notify Customer of any subpoena, judicial, administrative or arbitral order of an executive or administrative agency or other governmental authority ("Demand") that it receives, and which relates to the Personal Data unless prevented from doing so by law. At Customer request, Josys will provide Customer with reasonable information in its possession that may be responsive to the Demand and any assistance reasonably required for Customer to respond to the Demand in a timely manner.

5. **Data Subjects' Requests.**

5.1 Upon Customer's request and taking into account the nature of the applicable Processing, Josys will assist Customer by appropriate technical and organizational measures, insofar as possible, in complying with Customer's obligations under applicable Data Protection Laws to respond requests from Data Subjects to exercise their rights under applicable Data Protection Laws, provided that Customer cannot reasonably fulfill such requests independently, including through use of the Services.

5.2 If Josys receives a request from a Data Subject in relation to the Data Subject's Personal Data, Josys will notify Customer and advise the Data Subject to submit the request to Customer (but not otherwise communicate with the Data Subject regarding the request except as may be required by applicable Data Protection Laws), and Customer will be responsible for responding to any such request.

6. **Technical and Organizational Security Measures**. Josys will implement and maintain reasonable and appropriate physical, technical, organizational and administrative safeguards to preserve and protect the confidentiality, security, integrity, availability and authenticity of the Customer Personal Data against Security Incidents, including the security measures described in Annex B.

7. **Security Incident Notification**. In the event of any Security Incident, Josys will notify Customer without undue delay (but no later than 72 hours) after Josys becomes aware of the

Security Incident. In addition, Josys will also make reasonable efforts to identify the cause of the Security Incident and mitigate the effects to the extent within Josys' control. Upon

Customer's request and taking into account the nature of the processing, the information available to Josys, and any restrictions on disclosing the information such as confidentiality, Josys will assist Customer by providing information reasonably necessary to meet its Security Incident notification obligations under applicable Data Protection Laws.

8. **Audit Rights.** Upon 30 days' written notice by Customer and subject to the confidentiality obligations set forth in the Agreement, Josys shall make available to Customer its procedures relevant to the protection of Customer Personal Data in the form of Josys' third-party certifications and audit reports to the extent that Josys makes them generally available to its customers ("*Audit Report*"). Further, at Customer's written request, Josys will provide written responses (on a confidential basis) to reasonable requests for information made by Customer necessary to confirm Josys' compliance with this DPA, provided that Customer will not exercise this right more than once per calendar year unless Customer has reasonable grounds to suspect noncompliance with the DPA. In the event of a Security Incident, Customer shall have the right to request a copy of the most recent Audit Report, a Security Incident report, a remediation plan, and upon completion, a copy of a remediation plan showing any identified root cause remediated.

9. **Subprocessors.** Customer acknowledges and agrees that Josys may use the subprocessors identified in Annex C ("**Subprocessors**") to provide the Services and provides a general authorization to Josys to use Subprocessors. Customer further agrees that Josys may engage its Affiliates as Subprocessors. Customer may subscribe to receive automated notifications from Josys regarding any proposed changes to Subprocessors and give Customer an opportunity to object. Customer will have thirty (30) days from receipt of such notice to notify Josys of its objection to such Subprocessor by providing specific details of the objection based on reasonable data protection concerns. Josys shall respond to such objection within a reasonable time frame so long as such objections have a reasonable basis. Josys shall impose data processing and protection safeguards and measures substantially the same as set forth in this DPA on any Subprocessor prior to the Subprocessor Processing Personal Data. Josys remains responsible for compliance with its obligations of this DPA and for any acts and omissions of a Subprocessor that cause Josys to breach any of its obligations under this DPA.

10. **Deletion of Personal Data**.

10.1 During the Term. Josys will retain Customer audit logs for a maximum of 180 days, making them available for your use, access, and download (in CSV format). Josys may, at its sole discretion, delete Customer audit logs exceeding 180 days during the Term.

10.2 Post-Termination. Josys shall delete Customer Personal Data processed in connection with its provision of the Services within 180 days after termination of the Agreement, unless otherwise required by law. Notwithstanding the foregoing, back up files will be deleted within seven months of termination.

11. **CCPA.** In the event of Josys Processing the Personal Data of Data Subjects who are California

consumers under the CCPA, the required contractual clauses of the CCPA, as may be amended or replaced from time to time, are incorporated herein. Customer and Josys hereby acknowledge and agree that in no event shall the transfer of Personal Data from Customer to Josys constitute a sale of Personal Data or transfer of Personal Data for valuable consideration to Josys, and that nothing shall be construed as providing for the sale or transfer for valuable consideration of Personal Data to Josys. Josys shall not: (a) sell or share Personal Data; (b) retain, use, or disclose Personal Data for any purpose other than, and to the extent necessary to, perform the Services or as otherwise permitted by the CCPA; (c) retain, use, or disclose Personal Data for a commercial purpose that is not necessary to perform the Services unless expressly permitted by the CCPA; (d) retain, use, disclose, release, transfer, make available, or otherwise communicate Personal Data outside of the direct business relationship between Customer and Josys unless expressly permitted by the CCPA; or (e) combine Personal Data with personal information that Josys receives from or on behalf of another business or person, or that it collects from its own interactions with individuals. Furthermore, (i) the specific Business Purpose(s) for which Josys is processing Personal Data is contained in the Agreement and Josys acknowledges that Customer is disclosing the Personal Data to Josys only for the limited and specified Services set forth in the Agreement; (ii) Josys shall comply with all applicable sections of the CCPA, including (x) providing the same level of privacy protection as required of Customer by the CCPA with respect to the Personal Data as specified in Annex B (TOMs) and (y) reasonably assisting Customer in its obligations under the CCPA; (iii) to the extent required by the CCPA, and so long as there is a mutual agreement as to the scope of the monitoring in advance, Josys shall allow Customer or its designee (who shall not be a competitor of Josys and shall enter into an appropriate confidentiality agreement with Josys), upon 30-day notice during normal business hours, and at Customer's expense, monitor Josys' compliance with the CCPA specifically as to Customer's Personal Data; (iv) Customer has the right, upon written notice, to take reasonable and appropriate steps to stop and remediate Josys' unauthorized use of personal information; (v) Josys shall notify the Customer, should it determine that Josys can no longer meet its obligations with respect to Customer's Personal Data under the CCPA; and (vi) Josys and Customer shall enable each other to comply with consumer requests regarding the Personal Data which are made pursuant to the CCPA by forwarding any applicable consumer request made pursuant to the CCPA by email to Customer (in case of notice necessary to Customer) or to int-legal@josys.com if notice is necessary to Josys and provide the other party with any information necessary to comply with the request. Josys with the limitation of liability clause of the Agreement. For the avoidance of doubt, Josys' total liability for all claims from the Customer and all of its Tenants arising out of or related to the Agreement and DPA shall apply in the aggregate for all claims by Customer and all of its Tenants under both the Agreement and DPA, and, in particular, shall not be construed to apply individually and severally to Customer and/or to any Tenant, regardless of whether or not Tenant is a contractual party to the Agreement and DPA.

12. **Tenants.** Where a Tenant becomes a party to this DPA by its acceptance to the terms and conditions of the Agreement, it shall to the extent required under Data Protection Laws, be entitled to exercise its rights and seek remedies under this DPA, subject to the following: Except where Data Protection Laws require the Tenant to exercise a right or seek any remedy under this DPA against Josys directly by itself, the Parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such

remedy on behalf of the Tenant, and (ii) Customer as the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Tenant individually but in a combined manner for all its Tenants together.

13. **Limitation of Liability.**

The respective liabilities of Josys and Customer and its Tenants under this DPA shall be limited in accordance with the limitation of liability clause of the Agreement. For the avoidance of doubt, Josys' total liability for all claims from the Customer and all of its Tenants arising out of or related to the Agreement and DPA shall apply in the aggregate for all claims by Customer and all of its Tenants under both the Agreement and DPA, and, in particular, shall not be construed to apply individually and severally to Customer and/or to any Tenant, regardless of whether or not Tenant is a contractual party to the Agreement and DPA.

14. **Termination**. This DPA shall continue in full force until the expiration or termination of the Agreement or until Josys is no longer Processing any Personal Data of Customer.

15. **Miscellaneous.** If there is a conflict between any provision in this DPA and any provision in the Agreement, this DPA shall control with regard to the subject matter of this DPA. Except for changes made by this DPA, the Agreement remains unchanged and in full force and effect. This DPA shall be governed by and construed in accordance with the laws of the country of territory stipulated for this purpose in the Agreement, and each of the Parties agrees to submit to the choice of jurisdiction as stipulated in the Agreement with respect to any claim or matter arising under this DPA. In case a necessary provision is missing, the Parties shall add an appropriate one in good faith. In case of conflict, the order of precedence in respect of the Processing of Personal Data shall be this DPA and then the Agreement. If the Standard Contractual Clauses are an integral part of this DPA, then the Standard Contractual Clauses shall prevail. This DPA supersedes and replaces all previous written and oral agreements, communications and other understandings relating to the subject matter of this DPA.

ANNEX A
Details of the Processing of Personal Data

A. LIST OF PARTIES

Data Exporter(s):

1. Customer Name: As specified in the Order Form

Customer Trading Name (if different):

Customer Main Address (if a company registered address): As specified in the Order Form Customer's Official Registration Number (if any) (company number or similar identifier): Customer's key contact person's name: As specified in the Order Form

Key contact's position: As specified in the Order Form

Key contact's contact details: As specified in the Order Form Customer's DPO's name and contact information (if any):

Customer's EU Representative name and contact information (if any):

Activities relevant to the data transferred under these Clauses: Submitting data (which may include Personal Data) to the Services for Processing in accordance with the Agreement between Customer and Josys Inc.

Role: Controller or Processor

Data Importer:

1. Name: Josys (As set forth in Section 16.7 of the Agreement):

Main Address: (As set forth in Section 16.7 of the Agreement):

Official Registration Number (if any):

Key contact person's name, position and contact details: Head of Legal, int-legal@josys.com

Activities relevant to the data transferred under these Clauses: Processing data (which may include Personal Data) submitted by Customer's Users to the Services, and collecting Personal Data from Users of the Services, each for Processing in accordance with the Agreement between Customer and Josys.

Role: Processor

Categories of data subjects whose personal data is transferred:

The Personal Data transferred includes the following categories of data subjects:

1. Tenants of Customer and their employees, contractors and agents
2. Employees, contractors and agents of Customer

Any other data subjects' Personal Data submitted to the Services by Customer, Tenant or its service providers

Categories of personal data transferred:

1. Personal Data as determined by Customer
2. Telemetry and usage data including but not limited to username, user email address, password, device IDs, audit logs, Services features used, and error logs.
3. Support Authentication Data for provisioning of support services:
    - First and Last Name
    - Phone Number
    - Company Name
    - Title
    - Location (Country)
    - IP Addresses
    - E-Mail

Sensitive data transferred: None

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Continuous for the duration of the Services

Nature of the processing:

Collection, recording, analysis, structure, host, transfer, erasure, and any other activity Customer instructs the Services to perform on the Personal Data. Data Importer shall process Personal Data for purposes of the provision of Services to the Data Exporter, in accordance with the terms and conditions of this DPA and the Agreement.

Purpose(s) of the data transfer and further processing

As specified in the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As specified in the section titled "Deletion of Personal Data" in this DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

See Annex C– Subprocessor List – continuous for duration of the use of the applicable service.

ANNEX B

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Josys has implemented and shall maintain a security program that includes appropriate administrative, physical, and technical safeguards designed to protect Personal Data from Data Breaches and to help ensure the ongoing confidentiality, integrity, and availability of the Personal Data and Processing systems, taking into account the nature of the Personal Data that Josys processes and the risks involved.

The following sections describe Josys' current technical and organizational measures with respect to data security. Josys may change these measures at any time without notice, provided it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1. Access Control:

- **User Authentication:**
  - Multi-factor authentication (MFA) for all users accessing critical systems.
  - Role-based access controls (RBAC) to ensure that only authorized personnel have access to Customer Data.
  - Password policies: strong passwords with regular mandatory changes.
- **User Authorization:**
  - All services are configured with Principle of least privilege to safeguard critical data and systems from attacks.
- **Access Logs:**
  - Cloud Watch based detailed logging of access to sensitive Customer Data, monitored for anomalies.
  - Regular audits of access logs for suspicious activity.

2. Data Encryption:

- **In Transit:**
  - All data transmitted between customers and servers is encrypted using industry-standard TLS 1.2 (Transport Layer Security) protocol.
- **At Rest:**
  - Data stored in databases and storage systems like AWS S3 is encrypted using AES-256 encryption.
  - Encryption keys are managed using a secure key management system (KMS) with limited access. KMS utilizes symmetric AES 256-bit encryption.

3. Data Integrity & Retention:

- **Data Integrity Controls:**
  - Version control mechanisms to track changes to critical data.
- **Data Retention Policies:**
  - Data is retained based on business needs and legal obligations, following the DPA.
  - Customer Data is purged within 180 days after termination of the Agreement, adhering to SOC 2 Type II requirements.

4. Physical Security:

- **Data Center Security:**
  - **Tier 3+ Data Centers**: The SaaS infrastructure is hosted in AWS data centers, which meet or exceed Tier 3 standards. AWS data centers are certified for SOC 2 and ISO 27001, ensuring high standards of security and compliance.
- **Network Security:**
  - Robust firewall is in place to safeguard from potential threats.
  - Josys uses AWS services for Distributed Denial of Service (DDoS) Protection and Attack Mitigation.
- **Backup Facilities:**
  - Regular backups of all critical data, stored in AWS securely.
  - Backup systems undergo regular testing to ensure data can be restored quickly and securely.
- **Operational Security:**
  - **Contracting with Subprocessors:** Only sub-processors who have appropriate security measures and comply with data protection regulations are contracted.
  - **Training and Awareness**: Regular training and awareness programs for staff to ensure they are knowledgeable about security best practices and protocols and adhere to Josys' security procedures and practices.

5. Change Management:

- All changes to the SaaS application are submitted, managed and approved as change requests through the JIRA incident management system.
- Changes undergo comprehensive testing procedures, including unit testing, integration testing, and user acceptance testing, to ensure functionality, performance, and security.
- Quality assurance measures are applied to validate changes before deployment to the production environment.
- A rollback plan is defined and documented for each change to address potential issues or unforeseen complications during implementation.

- Stakeholders, users, and relevant teams are kept informed of planned changes through proactive communication channels, including status updates, notifications, and release notes.

6. Incident Management & Response:

- **Incident Detection & Response:**
  - Josys has 24/7 monitoring capabilities to ensure continuous surveillance of system operations, user activities, security incidents and environmental changes.
  - Automated alerts and notifications to detect anomalies, threshold breaches, and critical events in real-time.
- **Breach Notification:**
  - Detailed incident reports, scheduled maintenance notifications, and outage alerts are published to customers via the status portal.

7. Vulnerability Management & Penetration Testing:

- **Vulnerability Scans:**
  - Regular automated and manual vulnerability scans of both the infrastructure and application layers to ensure comprehensive security.
- **Penetration Testing:**
  - Semi-annual penetration tests by third-party security vendors to identify potential weaknesses.
- **Patching & Updates:**
  - Security patches for software and servers are applied promptly, following strict patch management procedures.

8. Secure Software Development (DevSecOps):

- **Secure Coding Practices:**
  - Code reviews include security checks for vulnerabilities, such as XSS (Cross-Site Scripting) and SQL injection.
- **CI/CD Security:**
  - Continuous integration (CI) pipelines are secured with automated security checks like Dependabot, Secret scan, NPM Audit scan, Lint scan.
  - Only approved code that passes security scans can be deployed to production.

9. Data Minimization & Privacy by Design:

- **Data Minimization:**
  - Only the minimum necessary Customer Data is collected and processed for the service.
  - Regular data audits performed to ensure unnecessary data is purged.

- An on-demand data purge capability is available, allowing customers to request immediate deletion of their data at any time.

- **Privacy By Design:**
  - **Proactive primary Measures:**
    - Privacy considerations are incorporated by design
      - Data is encrypted at rest and in-transit using high industry standards.
      - Role-based access controls and permission settings are implemented to restrict access to sensitive data

10. Technical Support Data Protection

- **Encryption**: Platforms used for technical support (HubSpot, Zendesk, FreshDesk, Jira, Slack) implement industry-standard encryption at rest and in motion, ensuring that Customer Data is protected during support interactions.
- **Access Control**: Access to support systems is restricted to authorized support personnel, with role-based access controls in place.
- **Data Handling**: Customer Data accessed during technical support is handled in accordance with this DPA, ensuring confidentiality and integrity.

11. Disaster Recovery & Business Continuity:

- **Business Continuity Plan (BCP):**
  - Routine testing of business continuity plans ensures minimal operational disruption in the event of a disaster.
- **Disaster Recovery (DR):**
  - Disaster recovery plan undergoes periodic testing to confirm service restoration within prescribed recovery time objectives.

12. Compliance & Certification:

- **Certifications:**
  - **SOC 2 Type II**: Josys is certified for SOC 2 Type II, demonstrating our adherence to stringent security, availability, and confidentiality standards.
  - **ISO 27001**: Josys is certified for ISO 27001, affirming our commitment to maintaining a robust information security management system (ISMS).
- **Audit Frequency:**
  - To maintain our SOC 2 Type II and ISO 27001 certifications, Josys undergoes rigorous audits at least once annually. These audits are conducted by independent, third-party auditors to ensure ongoing compliance with the required standards.

ANNEX C

LIST OF SUB-PROCESSORS

NAME	PURPOSE	DATA PROCESSED	LOCATION
Amazon Web Services	Hosting and storing of Customer Data, enabling scalability and availability of services	Customer Data, backup data, system logs	Japan
Hubspot	Managing Customer Data, marketing campaigns, sales automation, and Customer service interactions. Track leads, manage Customer accounts, and automate email marketing and sales workflows	Customer engagement data, interaction data	U.S.
Atlassian (Jira)	Tracking and managing Customer project tasks and issues	Customer project data, Customer issue tracking	Japan
Slack	Facilitating team communication and collaboration with Customers	Communication data, User information	U.S.
Pendo	Analyzing Customer interaction and engagement with the services	User engagement data, usage metrics	U.S.
Datadog	Infrastructure and application performance monitoring for the services	User engagement data, usage metrics	U.S.

GSuite (Google Workspace)	Managing Customer communication and document collaboration	User data, email content, documents	U. S.
Sales Force	Managing Customer Data, marketing campaigns, sales automation, and Customer service interactions. Track leads, manage Customer accounts, and automate email marketing and sales workflows	Customer engagement data, interaction data	Japan
Zendesk	Managing and responding to Customer support requests	Support tickets, user queries, contact data	Japan
OpenAI	Analyze Customer Data and User queries and generate content	Customer Data and User queries	U.S.
Raksul Vietnam Company Limited	Engineering resources	Maintenance support and support tickets	Vietnam

Josys may also engage one or more the following Affiliates as Subprocessors to deliver some or all of the Services provided to Customer:

NAME	**LOCATION**
Josys, Inc.	Japan
Josys Digital Technologies India Pvt., Ltd.	India