PURCHASING TERMS FOR ICT SERVICES

I. Applicability

1.1. This document forms part of the General Purchasing Terms of OVET B.V. (Client) and is declared applicable if, during the process of establishing a purchasing agreement with a supplier, it becomes apparent that ICT services are being procured which require specific information security requirements to be imposed on the supplier and its services.
1.2. Common principles of Security by Design are the foundation for the Client and therefore also for its suppliers in the development of software and systems.
1.3. Suppliers are required to report security incidents immediately to the Client's ICT department.

II. Software

If the Supplier provides or otherwise makes Software available, the following conditions apply:

2. License

2.1. Unless the Client pays for the use of the Software per time period, the Supplier grants the Client a **non exclusive, irrevocable, worldwide, perpetual, and unrestricted license** to use the Software. "Perpetual" means the license continues after the termination or expiration of the Agreement.
2.2. The Client may use the Software on separate systems for each of the following purposes: (i) testing, (ii) development/configuration, (iii) acceptance, (iv) business continuity, (v) backup, and (vi) disaster recovery.
2.3. The Client may use the object code of the Software without any restrictions, unless such restrictions are explicitly stated in the Agreement.
2.4. If the Client receives a copy of the object code of the Software, the Client may make an unlimited number of copies to distribute the Software within the organization. Ownership and copyright notices on the original copies must not be removed.

3. Documentation

3.1. The Supplier shall provide the Client with accurate, complete, and user-friendly documentation in Dutch or English regarding the features and usage of the Software.
3.2. The Supplier shall ensure the documentation remains up to date. The Supplier shall promptly update the documentation at its own expense if it is incomplete, unclear, outdated, or incorrect, and also if the Performance or equipment changes. The updated documentation shall be provided to the Client as soon as it becomes available.

4. Installation

a. The Supplier shall install the Software unless the Client indicates it will do so itself. Installation also includes migration and, if necessary, conversion of existing data files unless otherwise agreed.

b. If the Supplier knew or should have known that installation requires modifications to equipment or other software, the Supplier shall provide these as part of the agreed Performance.

5. Software Quality

5.1. The Supplier guarantees that the Software:

a. functions and will continue to function in accordance with the specifications and requirements in the Agreement (including the documentation) and the reasonable expectations of the Client; and

b. is free from material design and programming errors and does not contain any "backdoor," "time bomb," "trojan horse," "virus," "worm," or other code designed or intended to: (i) disrupt, disable, damage, or otherwise interfere with the operation of, or provide unauthorized access to, a computer system, network, or other device where such code is used, stored, or installed; and/or (ii) damage or destroy data or files without the Client's permission.

5.2. This warranty begins upon acceptance by the Client and remains valid for the duration of the Agreement and any extensions thereof.

5.3. The Supplier shall test the Software on the above points before delivery and only deliver it if it meets the requirements. If the Supplier is also responsible for installation and testing in the Client's environment, the Client shall provide a test environment.

6. Acceptance

6.1. The Client may conduct an acceptance test on the Software to verify whether it meets the Agreement and can be used in the production environment.

6.2. Acceptance of the Software occurs either through written confirmation by the Client or through use in the Client's production environment for more than one month without any malfunction, defect, or other issue. In case of partial delivery or systems consisting of multiple components, the Client may conduct interim acceptance tests of individual parts or components and a final acceptance test of the entire system once available. Acceptance does not exclude the warranty stated in Article 5.

6.3. If the Client does not accept the Software, the Supplier shall, at the Client's discretion:

(i) remedy the defects free of charge within 30 days, or

(ii) refund the fees paid by the Client for the Software.

Other rights and remedies under the Agreement remain unaffected. Upon receiving the corrected version of the Software, the Client may repeat the acceptance test.

7. Maintenance and Support

7.1. This article applies if maintenance of the Software has been agreed upon in a service agreement / service level agreement.

7.2. Supplier shall maintain a consistent version policy and share it with Client. New Versions and Releases shall be made available in a timely manner and contain at least the same

functionality as previous Versions and Releases. Client is not obliged to adopt a new Version or Release, and doing so shall not affect the warranties mentioned in Article 5.1.

7.3. Supplier shall ensure that the Software remains compatible with the Releases (including security fixes) of the operating system on which the Software is installed, as described by the platform provider as 'upward compatible'. Supplier shall also ensure compatibility with the operating system of any new platform replacing the original platform. A new Version or Release must not negatively affect the functionality of the Software or the platform, nor its proper and reliable operation.

7.4. Maintenance and support must not reduce the availability of the Software. If it is reasonably unavoidable that the Client cannot use the Software temporarily due to maintenance and/or support, Supplier shall request prior permission from Client and minimize the impact on Client's business operations.

7.5. To the extent the Software is intended to support compliance with laws and regulations, Supplier shall timely modify or supplement the Software in response to changes therein, ensuring continued compliance with the most recent laws and regulations.

8. Escrow

8.1. Upon Client's request, Supplier shall deposit the source code of the Software with an independent escrow agent under industry-standard conditions.

8.2. This agent shall release the source code directly to Client, without additional conditions and free of charge, if Supplier:

a. loses control over its assets or parts thereof, is declared bankrupt, or is granted suspension of payments;

b. ceases its activities without transferring its obligations under the Agreement to a Third Party;

c. fails to fulfill its obligations under the Agreement to such an extent that the intended use of the Software by Client is jeopardized.

8.3. Supplier shall ensure that the deposited Version of the Software is and remains identical to the Version used by Client. The release shall also include all information necessary for a reasonably experienced and qualified software developer to fully understand the structure of the Software. Supplier shall inform Client of each deposit.

8.4. After release, Client may use, improve, maintain, and develop derivative products from the Software without limitation. Client may also have these activities performed by its service providers.

III. Cloudservices

If Supplier provides Cloud Services, the following conditions apply.

9. Data en usage rights

9.1. All data processed by Supplier as part of the Cloud Services (Client Data) is and remains the property of Client. Client Data is confidential information. Supplier receives a non-exclusive, non-transferable right to use the Client Data and any Software provided by Client (Client Software) for the duration of the Agreement, solely to the extent necessary to perform the Agreement.
9.2. Supplier grants Client a non-exclusive, non-transferable, worldwide right to access and use the Cloud Services from any location during the term of the Agreement and any subsequent exit period. Supplier shall provide the necessary access keys and certificates to Client.
9.3. If Supplier provides Client access to third-party content or software as part of the Cloud Services, Supplier guarantees that it has obtained the necessary permissions from those third parties.
9.4. Supplier shall immediately inform Client of any request from government officials, regulators, or third parties for access to or delivery of data that includes Client Data. Supplier is obliged to refuse such requests and, in consultation with Client, to contest them.

10. Cloud Services Security

10.1 Supplier shall ensure that every physical and virtual service location is a secure environment accessible only to authorized personnel. If a connection is made between a service location and: (i) a system or network of Client, or (ii) the internet, Supplier shall ensure that such connection is secure and that unauthorized third parties cannot access the service location, Client's system or network, or Client Data.
10.2. Supplier shall continuously implement appropriate technical and organizational measures to secure Client Data and protect it against unauthorized or unlawful processing and accidental loss, destruction, or damage. Supplier shall also keep Client Data separate from other customers' data and ensure separation between the Software and the data server.
10.3. Supplier shall maintain an adequate and appropriate policy for backup, restore, and recovery of the Software and data required for the service, and ensure proper physical protection and access control to the Software and data in backups. Supplier shall perform at least one full recovery test annually and provide backup and recovery reports to Client upon request.
10.4. Supplier shall enable Client to store Client Data from Supplier's web server or similar mechanism in a format determined by Client to create its own backups. This does not relieve Supplier of its obligation to make sufficient backups of Client Data.
10.5. Before the start of the Service, the location (of the data server) where Supplier will store Client Data is known and approved by Client. This location may not be changed without prior written consent from Client.
10.6. Depending on the security risks associated with the provided Service, Client may agree with Supplier on a further specification of security measures and add this as an applicable addendum to the Agreement.
10.7. Client may conduct an external audit, including a penetration test, to verify compliance with applicable security requirements. Supplier is obliged to undergo such audit. An audit is not necessary if Supplier demonstrates the desired reliability of the service through certification (e.g., ISO27001, ISAE3402), or shows that an independent audit has taken place and shares the relevant results with Client (provided the scope of the certification matches the requested service).

11. Continuity of Service

11.1. Supplier shall implement continuity-protective measures against reasonably foreseeable incidents that could threaten the service and access to the Cloud Services. These measures shall ensure timely recovery of the service in case of major disruptions and safeguard the agreed service levels. Supplier shall document these continuity-protective measures and provide access to them upon Client's request.

11.2. Any incident for which Supplier has committed to implementing continuity-protective measures shall be fully attributable to Supplier. In such cases, Supplier cannot invoke force majeure.

11.3. Supplier shall not modify the Cloud Services in a way that results in reduced functionality or conflicts with Article 10.

12. Availability

12.1. Supplier shall always enable Client to retrieve Client Data and Client Software from the Cloud Services for at least ninety (90) days after the expiration or termination of the Agreement (and longer upon Client's request if necessary). The agreed service levels shall apply during this period.

12.2. Upon expiration or termination of the Agreement, Supplier shall provide all necessary support to Client to convert and retrieve the Client Data in a format agreed upon by the Parties, allowing Client to migrate and process the data in its own systems or those of an alternative provider.

12.3. Supplier shall destroy all remaining Client Data and Client Software in its possession in accordance with the most recent certified destruction standards, after (i) Client has successfully converted and retrieved the Client Data and Client Software from the systems used by Supplier to deliver the Cloud Services, and (ii) the Client Data and Client Software have been migrated and processed without errors or defects in Client's own systems or those of an alternative provider for a period of one (1) month. This obligation also applies to backups.