

End User Terms & Conditions

Provider: Cloud Services Group – CSG. is an Egyptian-based Software and IT Services company operating under the commercial laws and regulations of the Arab Republic of Egypt and holding commercial registration number 92133 – Egypt and is undertaking contractual agreements with customers and business entities under this agreement providing Software as a Service (SaaS).

AGREEMENT:

1. Definitions and interpretations

1.1 In this Agreement:

“Customer Materials” all works and materials:

(a) Uploaded to, stored on, processed using or transmitted via the Platform by or on behalf of the Customer or by any person or application or automated system using the Customer’s account; and otherwise provided by the Customer to the Provider in connection with this Agreement.

(b) Defect means a defect, error or bug having [an / a materially] adverse effect on the appearance, operation or functionality of the Software, but excluding any defect, error or bug caused by or arising as a result of:

(c) An act or omission of the Customer, or an act or omission of one of the Customer's employees, officers, agents, suppliers or sub-contractors; or

(d) An incompatibility between the Software and any other system, application, program or software not specified as compatible with the Provider's Software Products or Systems.

"Documentation" means the documentation produced by the Provider and [supplied / made available on the Platform] to the Customer specifying how the Platform should be used;

"Minimum Term" means the period that the Customer selects to subscribe in the Cloud Services Group selected Software as a Service Application.

Permitted Purpose means [define the purpose(s) for which the Platform may be used];

"Platform" means the software platform that is owned and operated by the Provider, and that will be made available to the Client as a service via [the internet] under this Agreement;

"SLA" means the Service Level Agreement made by the Provider to the Customer.

"Support Services" means support and maintenance services provided or to be provided by the Provider to the Customer in accordance with the Set Up services and customer/technical support services and commitments made by the Provider to the Customer according to the SLA commitments as enlisted and included in Schedule [1] of this Agreement.

"Term" means the term of this Agreement; and

"Upgrades" means new versions of, and updates to, the Platform, whether for the purpose of fixing an error, bug or other issue in the Platform or enhancing the functionality of the Platform.

2. Term:

The Term of this agreement is dependent on the number of months (Gregorian calendar) that the Customer selects to subscribe to according to the pricing of the CSG Software as a Service Applications made available on CSG Marketplace or made available to the customer in other mode of communication and agreed upon between the Customer and the Provider. Termination rights are made available to the Customer according to the Termination Clause set forth in this Agreement in Clause 12 of this Agreement.

3. The Software

3.1 The Provider will make available the Software to the Customer by [setting up an account for the Customer on the Platform, and providing to the Customer login details for that account] [as soon as practicable / and based on the successful completion of the Set Up of the customer's software based on the provider's Set Up schedule. 3.2 Subject to the limitations set out in Clause [3.3] and the prohibitions set out in Clause [3.4], the Provider hereby grants to the Customer a non-exclusive licence to use the Software for the Permitted Purpose [via any standard web browser / via [other means]] in accordance with the Documentation during the Term.

3.3 The licence granted by the Provider to the Customer under Clause [3.2] is subject to the following limitations:

[(a) The Software may only be used by the named users identified during the Set Up period with the customer providing that the Customer may change, add or remove a designated named user in accordance with the procedure set out therein.

(b) The Software granted to the customer by the provider over the cloud cannot be resold, reassembled, distributed or illegally provided to any other third party. All software usage by the customer is subject the provider's acceptance in writing to the customer.

3.4 The Customer must not use the Software:

(a) In any way that is unlawful, illegal, fraudulent or harmful; or

(b) In connection with any unlawful, illegal, fraudulent or harmful purpose or activity.

4. Support Services and Upgrades

4.1 The Provider may sub-contract the provision of any of the Support Services with obtaining consent from the customer.

5. Customer Materials

(a) The customer is entitled to all made available user documentation and user guide

6. Warranties

6.1 The Customer warrants [and represents] to the Provider that it has the legal right and authority to enter into and perform its obligations under this Agreement.

6.2 The Provider warrants [and represents] to the Customer:

- (a) That it has the legal right and authority to enter into and perform its obligations under this Agreement;
- (b) That it will perform its obligations under this Agreement with reasonable care and skill;
- (c) That the Software will operate without Defects and will perform substantially in accordance with the Documentation (subject to any Upgrades) and that any defects or low performance might arise from force-majeure issues not related to the technical infrastructure at the hands of the provider.
- (d) That the Software will be hosted in accordance with the requirements of the customer and will be available to the Customer in accordance with the Service Level Agreement commitments made by the Provider to the Customer and set out and included in Schedule [1] of this Agreement.
- (e) The Software (excluding for the avoidance of doubt the Customer Materials) will not infringe any person's Intellectual Property Rights.
- (e) The Software (excluding for the avoidance of doubt the Customer Materials) will not:
 - (i) Breach any laws, statutes, regulations or legally-binding codes;
 - (ii) Infringe any person's Intellectual Property Rights or other legal rights; or
 - (iii) Give rise to any cause of action against the Provider or the Customer or any third party,
- (f) The Software is and will remain free from viruses and other malicious software programs.

6.3 The Customer acknowledges that:

- (a) Complex software is never wholly free from defects, errors and bugs, and the Provider gives no warranty or representation that the Software will be wholly free from such defects, errors and bugs.
- (b) The Provider does not warrant or represent that the Software will be compatible with any application, program or software not specifically identified as compatible with the Provider's Software unless checked and approved by the Provider in writing to the Customer.

7. Security & Data Protection

The Provider's main role is to protect and enable the Customer to always have the upper hand and stay in full control and command over the business and operations data of the customer. The Provider

implements the following full security layers for the Customer's business and operations data that shall run over the Customer's Software:

CSG applies Security & Data Protection over four levels as follows:

Level 1: Infrastructure Security

- ✓ Network segmentation between Access Network and Management Network.
- ✓ Global security configuration against hackers and undesired access, spoofing, and the up-to-date security recommendations.
- ✓ Firewall monitored 24×7.
- ✓ Intrusion Prevention System configured to provide extra security level for the Internet requests.
- ✓ IPS automatically updated to protect the servers from the advanced and recent security breaches, OS bugs, applications security holes, port scanning, denial of service attacks and automatically block any suspicious and undesired requests.
- ✓ Datacenter access is controlled and monitored.

Level 2: Operating system Security

- ✓ Operating System security is maintained by following the vendor's security guidelines and best practices
- ✓ Security level is periodically updated by installing the critical hotfixes and security patches
- ✓ User accounts rights and permissions are carefully assigned to ensure maximum security
- ✓ File system permissions are optimized for best performance and maximum security
- ✓ Antivirus software installed to protect the operating system and all data files on the server from being infected.
- ✓ The Antivirus software has centralized management facility and gets automatic updates for the new virus definitions.
- ✓ The central Antivirus management generates virus alerts and allows immediate corrective action.

Level 3: Database Security

Database User Management

- ✓ The security administrator is the only user with the privileges required to create, alter, or drop database users.

Operating System Security

- ✓ Database administrator has the operating system privileges to create and delete files. Data Security Policy

- ✓ The security policy determines which users have access to a specific schema object, and the specific types of actions allowed for each user on the object.  Overall data security based on the

sensitivity of data. If information is not sensitive, then the data security policy can be more lax.

However, if data is sensitive, then a security policy is developed to maintain tight control over access to objects (prevent access to objects or encrypt data for sensitive table columns).

Database Procedures and Functions security policy

- ✓ All database procedures and functions encrypted by using oracle wrap utility.

Advantages of Wrapping PL/SQL Procedures

- ✓ By hiding application internals, the Wrap Utility prevents
- ✓ Misuse of your application by other developers
- ✓ Exposure of your algorithms to business competitors
- ✓ Wrapped code is as portable as source code. The PL/SQL compiler recognizes and loads wrapped

compilation units automatically. Other advantages include:

- ✓ Platform independence—you need not deliver multiple versions of the same compilation unit
- ✓ Dynamic loading—users need not shut down and re-link to add a new feature
- ✓ Dynamic binding—external references are resolved at load time
- ✓ Strict dependency checking—invalidated program units are recompiled automatically
- ✓ Normal importing and exporting—the Import/Export utility accepts wrapped files
- ✓ Protection for Connections as SYS and SYSTEM
- ✓ After database creation, the passwords for the SYS and SYSTEM are changed immediately.
- ✓ Application Developers and Their Privileges
- ✓ Specific system privileges granted to developers to restrict their overall capabilities in the database such as CREATE TABLE, CREATE PROCEDURE.

Level 4: Application Security

Basic Security Services

- ✓ **Authentication.** Allows a system to verify the identity of users and other systems that request access to services or data. Authentication is a prerequisite for many other security services, including access control, authorization, and accountability.
- ✓ **Authorization.** Allows a system to determine the privileges which users and other systems have for accessing resources on that system. Authorization is generally required for effective access control.
- ✓ **Access Control.** Ensures that a system grants access to resources only in ways that are consistent with security policies defined for those resources. Access decisions based on the authenticated identity and/or authorization of the requesting user, and on what type of access that user is requesting.

✓ **Data Protection.** Encryption mechanisms protect data sent through a public network from interception. Encryption also protects highly sensitive data (such as passwords) stored on a disk from users who bypass system access control mechanisms, such as by exploiting vulnerability in the underlying operating system or by stealing the physical disk storage medium.

8. Confidentiality

11.1 The Provider will:

- (a) Keep confidential and not disclose the Customer Confidential Information to any person or third party.
- (b) Protect the Customer Confidential Information against unauthorised disclosure by using the same degree of care as it takes to preserve and safeguard its own confidential information of a similar nature, being at least a reasonable degree of care; and
- (c) Without prejudice to the generality of Clause [12.1(b)], deploy and maintain the security systems and technologies to the Customer Confidential Information held on the Infrastructure of the Provider.

9. Termination

9.1 Either party may terminate this Agreement immediately by giving written notice to the other party if the other party:

- (a) Commits any [material] breach of any term of this Agreement, and:
 - (i) The breach is not remediable; or
 - (ii) The breach is remediable, but the other party fails to remedy the breach within [30] days of receipt of a written notice requiring it to do so; or
- (b) Persistently breaches the terms of this Agreement (irrespective of whether such breaches collectively constitute a material breach).

10. Effects of termination

10.1 Upon termination of this Agreement, all the provisions of this Agreement will cease to have effect, save that the following provisions of this Agreement will survive and continue to have effect (in accordance with their terms or otherwise indefinitely): Clauses [1, 7.5, 9, 10, 12, 14 and 17].

Customer commits under this Agreement that it shall fully pay and settle all related charges and

payments to the Provider resulting from the use and support obtained for the Customer's Software until the effective date of termination agreed upon between the Provider and the Customer. Customer understands that the Provider's minimum contractual period for a SaaS Application is a one (1) Year term based on Gregorian Calendar and effective from date of first invoice payment by the Customer to CSG – the Provider.

11. Force Majeure Event

The Provider does not warrant or guarantees to the Customer that the Software can work or perform the required operational performance expected by the Customer in the cases of "Force Majeure Events" such as, but not limited to: Power cuts, political crisis, natural disasters or violence around or near the Provider or Customer business premises. All the Software performance levels committed to the Customer are set forth under the SLA commitments to the Customer set forth in Schedule [1] of this Agreement.

Schedule [1]

SERVICE LEVEL AGREEMENT – SLA

1. Definition of SLA Support Item:

A) **Support Duration:** means the availability of CSG 1st and 2nd Line Support dedicated team to respond to partners and customers support tickets.

B) **Maximum Recovery Time:** means the time that client should expect their VM holding their application to come back to operation after an unprecedented shut down or breakdown in the Cloud Server/VM.

C) **Customer Support Response Time:** mean the time expected to respond back to partners and customers with a "resolution" on the reported/submitted customer issue/support request ticket.

2. SLA Types offered to Customers:

SLA Bronze

Support Item
Support Duration = 8 Hours per day – 5 Days a week
Maximum Recovery Time in case of Server Breakdown = Within 8 Hours from Breakdown Incident sta
Customer Support Response Time = Within 4 Hours from time of receiving Customer Support Reques

SLA Silver

Support Item
Support Duration = 16 Hours per day – 5 Days a week
Maximum Recovery Time in case of Server Breakdown = Within 4 Hours from Breakdown Incident sta
Customer Support Response Time = Within 2 Hours from time of receiving Customer Support Reques

SLA Gold

Support Item
Support Duration = 24 Hours per day – 7 Days a week
Maximum Recovery Time in case of Server Breakdown = Within 2 Hours from Breakdown Incident stai
Customer Support Response Time = Within 1 Hour from time of receiving Customer Support Request

