SERVICE LEVEL AGREEMENT

This Service Level Agreement (this “SLA”) is incorporated into the Service as a Subscription Agreement between Provider and Customer (the “SaaS Agreement”).
Terms defined in the SaaS Agreement and/or in the Terms of Services (the „ToS“) have the same meanings when used in this SLA. Further, as used in this SLA, calendar months and other timeframes are in the United Arab Emirates time zone, and business days and business hours refer to the period from 8:00 a.m. to 6:00 p.m. on any day except Saturday, Sunday, or any legal holiday in the United Arab Emirates

A. SOPE OF SERVICES TO BE COVERED

Detailed descriptions of every service offered. Service definitions can include how the services are delivered, an outline of the processes and a list of all technology and applications used. Exclusions. Specific services that are not offered should also be clearly defined to avoid confusion and eliminate room for assumptions from other party.

B. MONTHLY UPTIME

Solely to the extent Customer is not in breach of the SaaS Agreement and ToS, Provider shall issue a Credit to Customer if Monthly Uptime falls below 94,75% of the total minutes in any calendar month, based on the table below.

Monthly Uptime as a percent of minutes in the month	Credit: percent of that month’s System fees
94,75 % to 100%	0%
90% to 94,75%	10%
Below 90%	20%

As used above:

1. “Monthly Uptime” means the total minutes in the month minus the minutes of Downtime suffered during such month; provided Downtime of less than 10 minutes does not count for such purposes, in the aggregate or otherwise.
2. “Credit” means a credit against future Fees. Credits (a) do not apply to other amounts Customer may owe Provider, (b) apply to outstanding or future invoices only, and (c) are forfeit upon termination of the SaaS Agreement. Provider is not required to issue refunds or to make payments against Credits under any circumstances, including without limitation termination of this Agreement. To receive a Credit, Customer shall submit to Provider a detailed Credit request via email within ninety (90) days following the occurence of Error or Downtime (“**Timeframe**”). Customer’s failure to provide the request within the Timeframe will disqualify Customer from receiving a Credit.
3. “Downtime” means any period during which Customer cannot log into the SaaS, other than because of errors of Customer or its Users or failures of software or equipment operated by Customer or under its control or resulting from Customer’s and/or a third party’s software, network, links, products, services, widgets, apps, integrations, hardware or other equipment and/or resulting from Customer’s or anyone on its behalf use of the SaaS and/or the ServiceS in violation or in a manner not authorized in the SaaS Agreement or ToS; and/or (c) resulting from a Distributed Denial of Service (DDoS) attacks and/or other unlawful activity. Notwithstanding the foregoing, Downtime does not include: (a) Scheduled Maintenance; or (b) failures due to Force Majeure or any unavailability caused by circumstances beyond Provider´s reasonable control. Downtime begins when Customer submits a Trouble Ticket.
4. “Scheduled Maintenance” means any period of maintenance on the SaaS, provided Provider has given Customer 2 days’ notice of such maintenance.
5. “Trouble Ticket” means a written trouble ticket properly submitted through …………..

C. TRANSACTION PROCESSING TIMES

Provider shall issue a Credit (as defined above in Section B.2) of $5 for each user for each calendar day during which (1) average Transaction processing time exceeds 300 seconds or (2) more than 75% of Transactions are processed in 300 seconds or more.

D. ERROR RESPONSE AND REMEDY TIMES

Errors should be reported by Customer to Provider through any of the support channels listed below. An "**Error**" means any incorrect functioning of the SaaS and/or the Service that is reproducible, and which results in the failure of the SaaS and/or the Services to operate in full compliance with tshe functionalities set forth in the documentation. Provider shall define the severity classification of the reported Error and shall respond to the Error according to the response time set forth in the table below:

Severity	Description	Response Time
Critical	SaaS/Services Unavailability (as defined below).	Immediate but within 30 minutes
High	Major functionality in the SaaS/Service is impacted, or the Core SaaS functionality/ core Service performance is significantly degraded, or the Error is persistent and affects many Users. No reasonable workaround is available.	Immediate but within 1 hour
Medium	SaaS/Service performance issue or a material bug affecting some Users or some functionalities. Reasonable workaround is available.	Within 24 hours
Low	Bug or other technical issue affecting some Users. Reasonable workaround is available.	Within 24 hours

E. SUPPORT CHANNELS

All Provider´s support channels are available 5 days a week Monday to Friday,

Email support – Provider support team can be contacted through the contact form available Provider´s website or via the support email: support@arms.ae Customer has to make sure to contact Provider via Customer´s email registered with its Account.

Support within the system – a support icon allows the Users to open a ticket, join a webinar or look for answers in the knowledge base.
Training materials – training materials are available in the Provider´s website.

Self-service knowledge base – tutorials, guides and articles on anything you need to know about the SaaS/Service.

F. STAKEHOLDERS

Optional. Clearly defines the parties involved in the agreement and establishes their responsibilities.

G. BACKUPS AND DISASTER RECOVERY

For a permanent disaster impacting one server only, Provider´s Disaster Recovery Plan has the following metrics:

- RPO (Recovery Point Objective) = 5 minutes, i.e. can lose maximum 5 minutes of work

- RTO (Recovery Time Objective) = 30 minutes, i.e the service will be back online after maximum 30 minutes (Standby promotion time + DNS propagation time included)

For data center disasters (one entire data center is completely and permanently down), Disaster Recovery Plan has these metrics:

- RPO (Recovery Point Objective) = 24h, i.e. you can lose maximum 24h of work if the data cannot be recovered and we need to restore the last daily backup
- RTO (Recovery Time Objective) = 24h, i.e. the service will be restored from the backup within 24 hours in a different data center.

H. SECURITY

Provider's security strategy is to protect Customer Data at multiple levels, which includes data security, data integrity, and data privacy. Povider currently uses products by Oracle, Cisco Systems, Trend Micro, Veritas, ……..

To ensure the privacy, security, and availability of Customer Data and transactions, Provider employs the following technologies in delivering its service.

- Secure Data Center - Provider's production systems are located in one of the leading co-location facilities in the ……, Production web, application, and database servers along with network equipment are housed in a suite at the co-location facility which provides 24x7 security. To access the suite there are several levels of security that must be passed where each entry point provides state of the art card readers, scanners, and other access devices. Access to the facilities requires photo, encoded ID, and palm print.

- Encrypted User Authentication - Provider's users access the application using password authentication which is encrypted via 128-bit SSL. The robust design of the application prevents a customer from accessing another customer's data. There are several layers of protected servers that stand between the web page where the customer logs in and the actual data.

- Internet Firewalls - Provider's network is protected by redundant firewalls and monitored for unauthorized access. Firewall logs are constantly monitored, and the logs are reviewed on a regular basis. Leading-edge firewall equipment has been chosen to protect the network. The network has been architected to be highly reliable and redundant. If a router, load balancer, or firewall should fail, there is redundancy built in that would allow failover to take place, without causing a loss of service to Customer.

- Network Translation and Proxy Services
- Secure Socket Layer Data Encryption (SSL) - All web connections to Customer instances are protected with 256-bit SSL encryption (HTTPS with a 2048-bit modulus SSL certificate), and running behind Grade A SSL stacks. All our certificates chains are using SHA-2 already.

- Redundant, Highly Available Routers and Switches

- Redundant, Highly Available, and Secure Web and Application Servers

- Redundant, Highly Available Power

- Redundant, Highly Available Data Access

- Regularly Scheduled Backups, Offsite Storage

- Highly Available Application
- Secure Operating Systems - Provider uses tightly controlled passwords on its servers and network equipment. Provider limits access to production systems to authorized personnel

only. Passwords are changed on a regular basis. Security updates to the operating systems are tracked and updated as necessary.

- Data Security and Availability - Provider's uses 128-bit domestic and 64 bit international SSL encryption to protect the customer's data as it leaves our site. Provider uses ssh encryption via RSA (ssh1) and DSA (ssh2) public keys for communication between servers.

  Provider's OS and databases do not share the same passwords. Database users are restricted to a controlled list; individual activities are restricted, logged and monitored.
  Data is stored on highly redundant storage systems. The Oracle DB servers are configured in either a RAID 5 or RAID 1 (mirror) configuration. The main data, and archive and redo logs are written not only to this primary storage sub system on the server, but also written to network attached storage. The network attached storage has its own redundancy and is configured for cluster failover.
  Each customer owns his/her data and can export it from Provider, and the administrator user can export at any time. Customers can export their data from Provider by doing a CSV or IIF export.

Reliable Platform - Servers with full hardware guarantee, redundant data storage, network and electrical supplies, Provider looks at its application as well as the infrastructure as a tightly integrated system. All aspects of the system are designed to be reliable to ensure continued availability in the event that a component fails. All web and application servers are configured in a redundant manner. Provider has spare servers ready to deploy at a moments notice in the event of an equipment failure. The networking equipment is also configured in a manner to permit replacement equipment to be available within a few hours. NetSuite chooses equipment of the highest quality to power our application.
Passwords - Customer passwords are protected with industry-standard PBKDF2+SHA512 encryption (salted + stretched for thousands of rounds)
Safe Systems - Our servers are running recent Linux distribution with up-to-date security patches, with firewall and intrusion counter-measures (not disclosed for obvious reasons)
Isolation - Client data stored in dedicated databases - no sharing of data between clients, no access possible from one database to another.

I. DATA INCIDENT MANAGEMENT AND NOTIFICATION

Provider maintains security incident management policies and procedures and, to the extent required under applicable Data Protection Laws, shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data Processed on behalf of the Customer, including Customer Data transmitted, stored or otherwise Processed by Provider or its Sub-processors of which Provider becomes aware (a "**Data Incident**").

J. MISCELLANEOUS

Credits provide Customer's sole remedies and Provider's sole liabilities and responsibilities for Downtime, below-target Monthly Uptime, below-target Transaction processing speed, and below-target error Response and Remedy; provided this sentence does not restrict Customer's right, if any, to terminate the Agreement for material breach.

Under no circumstances is Provider required to issue Credits in excess of 60% of any calendar month's fees.

Provider may revise this SLA at any time by posting a new version at the SLA Website and providing written notice to Customer. However, during the then-current Term, Customer may reject any such revision that, on balance, materially reduces Customer's rights, provided Customer provides written notice of such rejection, disclosing the material reduction in detail, within 30 days of Provider's notice of the revision.