(SCHEDULE 4- SERVICE LEVEL AGREEMENT - FORMING PART OF APPENDIX 1 OF THE MASTER AGREEMENT)

(FOR INSTITUTIONAL CLIENTS)

MUBASHER FINANCIAL SERVICES (DIFC) LIMITED

OFFICE 303, LIBERTY HOUSE, DUBAI INTERNATIONAL FINANCIAL CENTER, P O BOX 507133, DUBAI

UNITED ARAB EMIRATES

(This Schedule 4 should be signed by Clients to cover service levels for GTNF)

GTN FRANCHISE ('GTNF') – SERVICE LEVEL AGREEMENT (SLA)

Account No:

Name of Account Holder (Client):

1 AGREEMENT OVERVIEW

This Service Level Agreement (SLA) is entered by and between Mubasher Financial Services (DIFC) Limited ('MFS' or 'Mubasher') and the Client as Schedule 4 to Appendix 1 and forms part of the Mubasher Brokerage Services Agreement dated…….. (Master Agreement).

The SLA outlines the parameters and service levels offered to support the GTNF as they are mutually agreed upon between MFS and the Client.

2 OBJECTIVE

The purpose of this SLA is to ensure that proper scope and commitments are in place to provide consistent and desired service to the Client by MFS.

3 SERVICE LEVELS

1. MFS agrees to ensure that GTNF will operate during market open hours in the relevant Financial Markets and provide an uptime guarantee of 98% on annual cumulative basis
2. MFS agrees to maintain similar standards in the DR site, as implemented and followed in the main datacentre, such as data integrity and confidentiality, datacentre site compliance and security controls.
3. MFS will provide user manuals and training to Traders, Users, Admin Staff, IT staff as required by the Client during the implementation phase of the GTNF.
4. All orders will be routed to the market on a first come, first served basis without any priority to any specific GTNF users. This will be applied to pre-market and regular market orders.
5. In case of any Dealer Terminal crash, rebooting of such terminal should not take more than one minute.
6. Any upgrade to the existing system will be rolled out to Client via a downloadable link or pushed directly to end-customers based on feasibility and availability of bandwidth.

MFS Initials Client's Initials

7. MFS undertakes to have in place required Business Continuity Planning (BCP) and Disaster Recovery mechanisms to ensure minimum service levels are maintained even during disruption to primary systems/operations. The BCP will be shared with the Client.

8. MFS will host, maintain, operate and run all Client's application data, services and processes, from a Tier-3 Etisalat hosting certified datacentre, running fully fault-tolerant components, at both the Main datacentre and DR site locations.

9. MFS undertakes to destroy all the personal data of Clients' "clientele base" on database level by running appropriate measures within 3 months after the service is terminated. MFS will update all customer's personal data with false data through a database query.

10. Client has the right to request and MFS is obligated to provide all required data, back in the required format, if the client decides to migrate to another system in the future

4 SECURITY SERVICES / PROCEDURES

1. MFS will provide bi-annual Vulnerability Assessment and Penetrating Testing (VAPT) report covering application security assessment and mitigation of High and Medium Vulnerabilities.

2. MFS will inform Client for any suspicious activities of data leakage and also provide admin and privileged user activity monitoring on end-customer information access.

3. MFS will report to the Client of any security incidents, breaches and/or suspicious activities at database and network level within 3 days after recovering from such incidents; and the same would be communicated over email

4. MFS will provide reports on security configuration changes on the application related to the client as and when these changes take place.

5. Confidentiality of Client information will be maintained at application, database and network levels using standard data security tools. The access to system will be limited through limited user access on a need to know and need to perform basis only and password controls.

6. MFS will maintain the integrity of Client information and data at both physical integrity through appropriate security of hardware and networking equipment as also logical integrity by ensuring the data is not subject to unauthorised changes including changes due to processing of the data, storage and transmission.

7. MFS will not use Client information stored on MFS system for any other purpose without written permission from the Client.

8. The Uniform Resource Locator (URL) for GTNF will be secured with a Secured Socket Layer (SSL) connection.

9. MFS undertakes to have Site-to-Site Virtual Private Network (VPN) connection for Admin Terminal between MFS and Client offices to ensure confidentiality of data transmitted between the two sites.

10. MFS undertakes to have an IT Policy covering Passwords, Information encryption, Information sensitivity, Risk assessment and Order Management System (OMS) credential request; the policy document will be shared with the client.

MFS Initials Client's Initials

11. MFS will implement advanced security controls for the Client's web facing applications, accessible through MFS's datacenters. The Security controls will include at a minimum:

    a. Web Application Firewall capable of protecting against vulnerabilities and exploits as described by the OWASP standard.
    b. Intrusion detection and prevention system
    c. Perimeter and Internal Firewalls, with multilayer segregation and defense in depth approach

12. MFS will support Client with any auditing requirements by providing the necessary logs and data related to application access and controls that are related to the client's data and hosting. These logs will include the following information,
    a. Web server logs
    b. Application server logs
    c. Databased logs
    d. Guest OS logs
    e. Host access logs
    f. Network Devices logs
    g. Application level logs
    h. Virtualization platform logs
    i. User Access records
    j. Management application logs

13. MFS will ensure that the Client's data is segregated at the application level so that the risks of data leakage with other Institutions is minimized.

14. MFS will put in place a structured and measurable approach to correctly identify, customize, implement, and repeatedly assess its security policies for accessing data.

15. . MFS will incorporate its own policies in terms of user access creation and data extraction, however, will seek prior permission from the Client before taking any action on this.

16. MFS will ensure Client's data protection in all legal scenarios where MFS could be party to any legal issue such as acquisition, merger, bankruptcy, regulatory action and/or suspension, which could potentially directly or indirectly affect Client's operation and Client's data privacy protection. MFS shall in such cases assist the Client with accessibility and availability of its data by liaising with the concerned regulatory authorities

17. MFS will implement security patches in a timely manner.

18. Client can visit MFS Head Office by a pre-arranged meeting between the two parties

5 CHANGE MANAGEMENT PROCEDURES

1. MFS will agree to Change Request (CR) on the system by the Client as long as the changes do not affect the performance of MFS systems and also do not affect other existing customers of MFS, and this should be approved by MFS team to implement.

2. Any Change Request (CR) from the Client will be assessed by MFS technical team internally and the Client will be informed about the outcome of assessment and charges applicable for the change, if any. Once informed, the Client may agree/disagree with the assessment. If agreed, MFS team will proceed with CR implementation. If disagreed, the CR request will be closed.

MFS Initials Client's Initials

3. Any Change Requests (CR) from market side specific to the exchange which does not affect MFS current business/customers or Client business will be analysed, developed, tested and implemented without additional charges provided internal approvals are given by MFS Management

4. MFS will notify Client over email as and when the CR has been rolled out to production.

6 SERVICE REQUESTS

All concerns related to GTNF must be initiated through Client by email to MFS and can be followed up on with a phone call by Client to the Point of Contact (POC) of MFS, the details of whom are given in Schedule-3. After receiving the email from Client and registering the problem, MFS will send a response confirmation email.

7 ROLES AND RESPONSIBILITIES

1. Client is the "data owner" of all data that is created, modified, used and archived within the MFS system, for the Client's business, and as a result of this Client is also the "data controller".

2. As owner of its Data, the Client will have the right to request and obtain any data it requires along with the relevant metadata information, from MFS, without limitations on the size or granularity of the data.

3. MFS will ensure that Client's data, at its most granular level, will be preserved and maintained for access on a long-term archival basis based on Regulator's policy applicable on the Client and MFS.

4. MFS is the "data custodian" of the Client's data, and will ensure optimum protection of the data from illegal and unauthorized use and access. Upon termination of this agreement, MFS will provide a copy of the Client's data to the Client. Subsequent to Client having received its data, MFS shall arrange to delete such data from its database and confirm to the Client of such deletion.

8 CONTACTS AND ESCALATION

Escalation matrix document covering below details will be separately shared through email

1. Network Support
2. Application Support

9 DATACENTER AND DATA STORAGE LOCATIONS

Primary Datacentre: Dubai, UAE Zabeel datacentre
DR Datacentre: Dubai, UAE, TCN datacentre

MFS Initials Client's Initials

10 ACCOUNTABILITY

1. MFS plans to retain an IT auditing provided by a third-party company. Once the IT auditing is finalized MFS will inform the client, and will be sharing the IT auditing reports with the client. As mentioned in point 12 under security services and procedures, MFS will support the client during the client's auditing period.

2. MFS will be sharing VAPT (vulnerability assessment and penetration testing) reports with the client annually after finalizing the tests

3. MFS will inform the client of any system maintenance procedures, if the maintenance procedures requires a cutoff of the service MFS will cutoff the service outside the business hours, and will inform the client about the duration of the cutoff and will inform the client when the service is available after the maintenance.

IN WITNESS WHEREOF, the parties hereto have executed this Service Level Agreement on the date herein below written.

For **Mubasher Financial Services (DIFC) Limited**	For
BY: _____	BY: _____
NAME:	NAME:
Designation:	Designation:
Date: / /	Date: / /

****

MFS Initials

Client's Initials