MFSA MALTA FINANCIAL SERVICES AUTHORITY

Live Audit Log
GUIDELINES

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

CONTENTS

REVISIONS LOG

VERSION	DATE ISSUED	DETAILS
1.00	15 OCTOBER 2021	DOCUMENT ISSUED

Title 1 General

Section 1 Scope and Application

G1-1.1.1 The aim of this document is to provide guidelines and specify the requirements for the Live Audit Log ("LAL") as per R3-2.1.6.1 of Chapter 3 of the Virtual Financial Assets ("VFA") Rulebook ("the Rules").

G1-1.1.2 These Guidelines shall be applicable to:

i. VFA Service Providers licensed by the MFSA under the VFA Act (hereinafter 'LHs')

G1-1.1.2 These Guidelines are applicable as of date of publication.

Section 2 Overarching Principles

G1-1.2.1 A VFASP shall ensure that:

i. it can continuously be in a position to provide the data as specified within the Data Requirements section ("the Data") without undue delay, as and when required by the Authority;
ii. the Data is continuously kept complete, up-to-date and faithful to the original events;
iii. the necessary measures are in place to ensure the confidentiality, integrity and availability of the Data at all times.

These guidelines are without prejudice to the relevant Acts, Regulations, Rules and/or sector-specific guidelines including the Act and the Innovative Technology Arrangements and Services Act.

The burden of proof for compliance with the requirements set out within these Guidelines remains with the VFASP at all times.

Title 2 Data Requirements

Section 1 LAL Data

G1-2.1 The LAL shall hold a log with all transactions taking place as part of the LH's Licensable Activity. As a minimum, transaction logs need to contain the following data:

Sub-Section 1 Transaction Data

Field name	Type	Description	Valid values
TransactTime	TIMESTAMP	Time in UTC when the trading instruction (i.e. new order, order cancel etc.) was created in the trading system, or when a fill happened	
Id	String	Order ID assigned to the order	
Version	int	Version of the order as the state of the order change with different transactions	
Symbol	String	Pair name to trade. Ex: BTC/EUR	<base/counter>
Side	String	Side of order	Buy Sell
OrderQty	String	Number of units	
Price	String	Price per unit on Limit order	
OrdType	String	Order Type	Market Limit StopLoss
OrdStatus	String	Identifies current status of order, note that: 0=Accepted D=New	Accepted PartiallyFilled Filled DoneForDay Canceled Replaced PendingCancel Stopped Rejected Suspended PendingNew Calculated Expired PendingReplace New OrderCancelRequest OrderReplaceRequest
ExVenue	String	Venue name which provided the execution	
AvgPx	String	Broker calculated average price of all fills/executions on the current order. Will be	

		available on part filled/filled orders	
CumQty	String	Total quantity filled	
LeavesQty	String	Remaining, unfilled/uncanceled quantity on the order	
TimeInForce	String	Specifies how long the order remains in effect	Day GoodTillCancel AtTheOpening ImmediateOrCancel FillOrKill GoodTillCrossing GoodTillDate AtTheClose
ExpireDateTime	timestamp	Date of order expiration	
OrderCapacity	String	Designates the capacity of the firm placing the order	Agency Proprietary Principal
Account	String	Field used for account mnemonic. Its identification source is mutually agreed between the counterparties	
ClientId	String	Unique identifier of the client/beneficiary of the order. Represented in fix as part of PartyRole <452> and PartyID <448>	Client ID <Client ID>
OriginationTrader	String	Buyside firm associated with Order Origination Firm which originates/submits the order.	
LastLiquidityInd	String	Indicator to identify whether this fill was a result of a liquidity provider providing or liquidity taker taking the liquidity.	AddedLiquidity RemovedLiquidity LiquidityRoutedOut

Sub-Section 2 On Chain Data

Field name	Type	Description	Valid values
TransactTime	TIMESTAMP	Time in UTC when the transaction happened	
ORIWallet	String	Originator wallet address	
BENWallet	String	Beneficiary wallet address	
TXID	String	Transaction ID/Hash	
Currency	String	Currency symbol Ex: BTC	
Quantity	float	Total units currency	
Type	String		Deposit Withdrawal
ClientId	String	Unique identifier of the transaction creator.	
TravelRule	String	Presence of Travel rule information attached to the transaction	Yes No NA

Sub-Section 3 System Log Data

G1-2.1.3 Application, Database, Operation and Security Log Data generated by the Arrangement (duration).

Section 2 Data retention

G1-2.2 Log data shall, as a minimum, be retained within the LAL for a period of <5> year(s) from the date of the log data. The Authority may require a LH to retain any data for a longer period of time under particular circumstances (e.g., an investigation) within the same LAL or within an arrangement compliant with the requirements set out within these Guidelines.

LHs shall ensure that they adhere to their obligations under the General Data Protection Regulation and any other applicable Acts, Regulations, Rules and/or sector-specific Guidelines.

Depending on the trading capacity of the LH and whether or not the LH is dealing for a client, a transaction may have to be reported in more than one report.

Section 3 Data Synchronisation

G1-2.3 The Data should be made available on the LAL on a "T+1" basis, or at most, 24h after the relevant transaction or event, as the case may be, takes place.

Section 4 VFA Services specifics

Sub-Section 1 Reception and transmission of order(s)

G1-2.4.1 Where a LH is receiving and transmitting orders on behalf of Client on a trading venue, the LAL should be populated with market side data.

Sub-Section 2 Execution of order(s)

G1-2.4.2 Where a LH is executing orders on behalf of Client on a trading venue, the LAL should be populated with market side data.

Sub-Section 3 Dealing on own account

G1-2.4.3 Where a LH is dealing on own account by automatically taking the other side of a trade it should be reported as principal under Order Capacity. Example: If a client is a buyer, the LH is selling from their inventory. If the client is a seller, the LH is adding to their inventory.

Where a LH is trading on its behalf, it should be reported as Proprietary under Order Capacity. Example: a proprietary trader decides what to buy/sell and when using their own discretion.

Title 3 Operational requirements

Section 1 Hosting requirements

G1-3.1 The Arrangement including the Data shall be:

1. located/based/hosted in EU/EEA. LHs shall ensure that a self-contained instance of the LAL including a complete and up-to-date instance of the Data is located/based/hosted in EU/EEA;
2. hosted in a Tier 3 data centre or above;
3. hosted in a data centre that is ISO/IEC 27001 certified or equivalent;
4. hosted on dedicated hardware. If the LAL is designed to entail virtualisation, the hardware hosting the Arrangement shall be dedicated solely to the LAL;
5. available and accessible to the LH at all times.

Section 2 Management practices requirements

G1-3.2 LHs are required to demonstrate that they employ / have employed, sound management practices to adequately plan, design, build, operate and continually improve the LAL.

LHs shall particularly ensure that the following practices are employed and documented:

1. Asset, Configuration and Change Management;
2. Risk Management;
3. Information Security Management;
4. Availability and Continuity Management;
5. Capacity and Performance Management;
6. Monitoring and Event Management;
7. Incident and Problem Management;
8. Outsourcing Management;

LHs shall refer to the Guidance on Technology Arrangements, ICT and Security Management and Outsourcing Arrangements and may consult other standards and best practices.

LHs shall ensure that the LAL is included in the scope of the IT Audit by auditors with sufficient knowledge, skills and expertise to provide assurance to the LH's Management Body that the Arrangement is compliant with the requirements set out within these Guidelines and as to the effectiveness of the controls in place.

Section 3 Operational processes requirements

G1-3.3 Without prejudice to any other operational requirements, LHs shall employ and are required to demonstrate that they employ operational processes that support the required management practices in Section 04. For instance, LHs are required to have processes for Asset Configuration and Change Management, backup processes that support Availability and Continuity Management, and a process for Incident Management. Such processes need to be documented in line with the requirements of Section 07.

Section 4 Information Security requirements

G1-3.4 Without prejudice to any other operational requirements, LHs are required to demonstrate that they employ sound information security management

practices to ensure the Confidentiality, Integrity and Availability of the Data. LHs shall particularly ensure that the following practices are employed and documented:

1. Background verification of personnel having physical and/or logical access to the Arrangement;
2. Protection from unauthorised physical and logical access complemented by access control policies;
3. Physical access controls complemented by defined physical access procedures, surveillance of the physical aspect of the arrangement using cameras, physical access registers;
4. Logical access controls complemented by defined roles and responsibilities, segregation of duties, logical access procedures, access and privilege management, secure log-on procedures;
5. Protection from malware and/or other malicious software;
6. Protection of the Arrangement in general (confidentiality, integrity and availability) and the Data in particular in its different states (e.g. at rest, in transit) against unauthorised/unlawful access, modification, processing, and loss;
7. Operational and Security Monitoring including file integrity monitoring;
8. The enablement of the required system log data (refer to Section 02) and the transmission of such log data to a separate log data repository, including measures to manage data manipulation risks (intentional or unintentional);
9. Sound Key Management practices for cryptographic controls complemented by recommendable key-lengths;
10. Security testing (including penetration testing) complemented by regular vulnerability and patch management;
11. Secure configuration baselines and hardening in line with reputable standards, enabling what is strictly necessary (e.g. system processes and services);
12. Accurate Time Synchronisation (applicable across all the architecture and traceable to an Accurate Time Source);
13. Adequate backup processes including regular testing.

Section 5 Documentation requirements

G1-3.5 Without prejudice to any other documentation requirements, LHs shall have the following documentation available and up to date at all times applicable to the LAL:

1. Documented processes and/or procedures as applicable covering the requirements set out within these guidelines;

2. A detailed and comprehensive architectural blueprint (including the Data) of the LAL and how it relates to the overall architectural blueprint of the Licensable Activity;
3. An inventory of assets (hardware, software, data) of the Arrangement;
4. The configuration of the assets and their inter relationship;
5. The capacity and performance of the arrangement, including storage and performance forecasts;
6. The information security controls (refer to Section 06);
7. A change log which shall as a minimum, for each change, include the date and timeframe, the rationale, a risk assessment including any back-out plans, details and steps undertaken, the assets involved, the implementor/s, approval by the management body, and whether an emergency change or not;
8. Identified risks and risk management strategies associated with the LAL as part of the overall risk management framework of the LH;
9. The outsourcing arrangements and third parties associated with the Arrangement (the LH remains accountable for the Arrangement at all times);
10. An Incident Log which shall as a minimum, for each incident, include the date and time of discovery, the actual date, time and duration, the impact, the root cause, and the resolution.
11. Disaster Recovery Procedures in line and in conjunction with high availability requirements, defined Recovery Time Objectives and Recovery Point Objectives, and a record of all regular testing carried out;
12. As part of the set of documented operational procedures, the procedure to provide access/the Data or extracts thereof to relevant authorities and, or law enforcement agencies upon order or request.

Section 6 People requirements

G1-3.6 The LHs shall identify a person with the necessary seniority, skills, knowledge, and experience to ensure that any request for information regarding legal compliance and the operational behaviour of the system can be acted upon satisfactorily. Such person shall assume responsibilities of a Technical Administrator.

As per R3-2.1.6.2 of the Rules, the LH shall notify the MFSA prior to the appointment or replacement of the person referred to in R3-2.1.6.1 of the Rules.

Technical administrator

A Technical Administrator must satisfy the following criteria:

- be of good conduct;
- demonstrate that he/she has the relevant qualifications and experience within the technology field of the LAL;
- have sound knowledge of the applicable laws, standards, regulations and guidelines relevant to the Technical Administrator and the LAL;
- provide proof of sufficient technical resources as an individual, through delegates, or with third party support to meet operational and compliance obligations and to meet the Authority's requests.
- Resident of Malta

Section 7 Data Extraction and Reporting requirements

G1-3.7.1 LHs are expected to make use of the transaction reporting templates (Off-chain and On-chain) available on MFSA's website and follow the below naming convention:

- YYYYMMDD_LHCode_ONC-1 *for On Chain data*
- YYYYMMDD_LHCode_OFFC-1 *for Off Chain data*

As a reminder, LH Code can be found in the Financial Services Register on MFSA's website.

To adhere to G1-2.3, two .csv files (one for On Chain data & one for Off Chain Data) should be created per day and stored on the Live Audit Log.

In the event where a second .csv file is required, the last digit in the name shall read "2" (e.g., YYMMDD_LHCode_ONC-2 for On Chain data).

LHs should keep abreast of any updates issued by the MFSA and ensure that they are using the latest version available.

G1-3.7.2 The Authority may, from time to time, request LAL data accordingly. In this respect, following such a request, LHs are expected to cooperate with the Authority and provide the requested data within the stipulated timeframe. Non-compliance to this requirement might result in regulatory actions.

Moving forward, the MFSA may define interface / integration standards (e.g., though APIs) for remote extraction of the Data from the LAL. LHs shall keep this in mind within their planning and design stages of the LAL.

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

Malta Financial Services Authority
Triq L-Imdina, Zone 1
Central Business District, Birkirkara, CBD 1010, Malta
communications@mfsa.mt
www.mfsa.mt