Guidelines for Vault Manager by Bullion Depository

(Pursuant to Clause 3 & 4, Section III of the IFSCA Operating Guidelines vide Circular No. F. No. 415/IFSCA/Consolidated Operating Guidelines/2021-22 dated August 25, 2021)

1. Vault Security and Access Control Systems

The Vault Manager shall ensure implementation and maintenance of robust vault security and access control systems, including but not limited to the following:

1.1 Physical Security Measures:

1.1.1. 24/7 CCTV surveillance with recording / storage capability of surveillance data in the DVR should be adequate and meets international standards say for a period of minimum one year.
1.1.2 Access to vault premises must be restricted to authorized personnel only, with entry logs maintained.
1.1.3 Biometric or dual-authentication access control systems at all entry points of the vault areas.
1.1.4 Vault area perimeter security including alarms, motion detectors, reinforced wall and strong access doors.
1.1.5 Security guards and physical rounds as required.

1.2 Access Authorization Protocol:

1.2.1 Access must be granted on a "need-to-access" basis only.
1.2.2 Emergency access must be logged, reported and justified.

Guidance Note - The vault manager shall ensure that access to the vault is secure, traceable, thereby reducing the risk of unauthorized or inappropriate access.

2. Systems for Tracking Commodities

The Vault Manager shall implement a comprehensive digital system for end-to-end tracking of bullion stored, transferred or withdrawn. The system must include but not be limited to:

2.1 Inventory Management System (IMS):

2.1.1 Real-time updates of bullion inventory in the vault.
2.1.2 Assignment of unique identifier codes to each bullion unit for easy identification.

2.2 Daily Reconciliation:

2.2.1 Physical and electronic inventory to be reconciled daily.
2.2.2 Discrepancies, if any, must be immediately reported to the Bullion Depository (IIDI).

2.3 Logistics:

2.3.1 The security provided to bullion during transit or in loading and dispatch areas should be as comprehensive as that of bullion in vault for purposes of taking into account the risk of transit outside premises.
2.3.2 Delivery and loading areas must have restricted access, surveillance and logging to ensure secure and controlled bullion movement.
2.3.3 Implement processes for secure movement, verification and reconciliation of bullion while sending across all locations.
2.3.4 Real-time tracking of bullion inventory during in-transit.
2.3.5 Formal logistics movement policies, procedures and control shall be in place to protect the transfer of assets using all types of communication and tracking facilities.

Explanation - The vault must have formal, documented policies and procedures for the secure transfer of bullion, covering authorization, transport and tracking. All movements should use secure communication and tracking systems, such as GPS, RFID or digital updates, and employ tamper-evident packaging. Every transaction must be logged, monitored and reconciled to ensure accountability, traceability and compliance with regulatory requirements.

3. Risk Control and Operations Manuals

Vault Manager must establish, document and maintain operational and risk control manuals, which must include but not be limited to:

3.1 Risk Control Manual:

3.1.1 Risk Identification: Security breaches, operational lapses, natural disasters, cyber threats, theft, fire, burglary, etc.
3.1.2 Risk Assessment: Quantification of risk exposure.
3.1.3 Risk Mitigation Measures.
3.1.4 Regular drills and training.
3.1.5 Adequate Insurance coverage for stored bullion in line with IFSCA operating guidelines.
3.1.6 Dual verification (maker-checker functionalities) for all transactions.

3.2 Operations Manual:

3.2.1 Standard Operating Procedures (SOPs) for:

3.2.1.1 Bullion receipt, verification and deposit.
3.2.1.2 Bullion withdrawal and delivery.
3.2.1.3 Bullion auditing and inspection.
3.2.1.4 Incident Reporting Procedures.
3.2.1.5 Roles and responsibilities of vault personnel.
(*Enclosures: Copies of Risk Control and Operations Manuals are to be provided as annexures to the Bullion Depository (IIDI).*)

4. Independent Internal Control Mechanisms

The Vault Manager shall institute internal control mechanisms to ensure transparency, accountability and compliance, which shall include:

4.1 Internal Audit Function:

4.1.1 Independent internal audit to be conducted on a yearly basis.
4.1.2 Reports to be submitted to the Bullion Depository.

4.2 Control Framework:

4.2.1 Segregation of duties to prevent conflict of interest.
4.2.2 Maker-checker validation for all data entry and transaction processes.

4.3 Monitoring & Evaluation:

4.3.1 Key Performance Indicators (KPIs) and compliance checklists.

Explanation - The vault manager has to define measurable KPIs covering critical operational, risk management, security and compliance aspects of vault operations, including but not limited to turnaround times, inventory accuracy, incident reporting, audit observations and adherence to standard operating procedures.
The vault manager shall establish KPIs and compliance checklists aligned with applicable IFSCA regulations and internal policies to monitor operational, risk, security and compliance performance.

4.4 Reporting Systems:

4.4.1 Periodic reporting to the Bullion Depository on inventory, incidents and audits.
4.4.2 Immediate reporting of any material deviation or breach to the Bullion Depository (IIDI).

5. Hardware, Software, and Communications Systems: Details of Capability, Function, and Location

5.1 Vault Managers shall maintain comprehensive and up-to-date documentation encompassing all hardware, software, and communication systems. Such documentation must include system capabilities, functions performed, and physical or virtual locations. Additionally, appropriate controls shall be implemented to secure these systems against unauthorized access and ensure their integrity.

Directives include but are not limited to:

5.1.1 Maintain detailed diagrams and inventories of all relevant IT and communication infrastructure.
5.1.2 Implement and document the safeguards of endpoint devices and software configurations.
5.1.3 Establish strict access control measures with logs maintained for review and audit.
5.1.4 Enforce physical security controls to prevent unauthorized physical access to critical systems.
5.1.5 Ensure secure hosting environments for applications supporting Bullion related operations.

Explanation - The Vault Manager shall ensure that the IT systems used for all operational activities, whether provided by the Depository or otherwise, are adequately secured, regularly updated and maintained with appropriate controls, access management and audit trails. Necessary safeguards shall be implemented to ensure system integrity, data security and operational resilience so as to mitigate the risk of any unforeseen events.

6. Data Storage and Backup Procedures: Details of Capability, Function, and Location

1.1 Vault Managers must establish and document data storage solutions and backup procedures that guarantee data integrity, availability, and confidentiality. Backups should maintain data integrity and shall be protected and resilience against data loss and stored in geographically separate, secure locations.

Directives include but are not limited to:

1.1.1 Maintain documented data storage and backup policies consistent with regulatory retention requirements.
1.1.2 Implement secure backup procedures, including off-site storage to mitigate risks of data unavailability.
1.1.3 Ensure audit trails, access logs and other critical records are stored, securely backed up and accessible any time. Logs of all physical access attempt shall be securely maintained, and failed access attempts shall be reviewed.

1.1.4 Maintain appropriate retention periods for all data, logs, audit trails, including surveillance records, as mandated by applicable legal and regulatory requirements.

Explanation - The Vault Manager shall ensure secure storage and backup of all operational data, irrespective of the system used, so as to maintain data integrity, confidentiality and availability and to prevent any data loss. Backup systems shall have appropriate access controls, audit trails and data retention in accordance with applicable laws, regulations and directions of the Authority, and shall be available for audit or inspection as required.

7. Disaster Recovery Systems and Procedures

7.1 Vault Managers are required to establish robust disaster recovery systems and procedures to ensure business continuity and rapid restoration of critical operations in the event of an incident. These procedures must be formally documented, regularly tested, and updated to address evolving risks.

Directives include but are not limited to:

7.1.1 Develop and maintain a formal disaster recovery plan covering data restoration, system recovery, and business continuity of operations.
7.1.2 Conduct periodic testing of recovery procedures to validate effectiveness and identify areas for improvement.
7.1.3 Ensure that findings from security assessments and audits are integrated into disaster recovery planning.

8. Data Retention & Retrieval

8.1 All records, books of accounts, access logs, audit trails and transaction data shall be preserved as per the specified standards or as mandated by IFSCA from time to time.
8.2 Vault Manager must establish a secure and searchable data archiving system with role-based access.
8.3 Retrieval of records for the past twelve months must be possible within 24 hours of a request from the Bullion Depository, Regulator or any Authority. Retrieval of records beyond the past twelve months must be completed within an extended timeframe of 72 hours from such request.