INFORMATION SECURITY AND DATA PROTECTION POLICY

Company	**GoldTakas FZCO**
Jurisdiction	United Arab Emirates – Dubai / DMCC
Version / Date	2.0 / 28.08.2026
Effective Date	01/09/2026
Document Owner	MLRO / Compliance Function
Approval Authority	Senior Management

This Policy shall be read in conjunction with GoldTakas FZCO's Code of Ethics and Business Conduct Policy, AML/CFT Policy, Client Acceptance Policy, Whistleblowing Policy and other applicable internal procedures.

Rather than duplicating operational IT procedures, this Policy establishes the principles, responsibilities and controls relating to the protection of information assets, Confidential Information and Personal Data processed by GoldTakas FZCO.

1. PURPOSE

The purpose of this Policy is to establish a framework for protecting information assets, Confidential Information and Personal Data against unauthorized access, disclosure, alteration, loss, misuse or destruction.

GoldTakas FZCO recognizes that information security and data protection are essential to maintaining client trust, regulatory compliance and operational resilience.

This Policy aims to:
• Protect Confidential Information and Personal Data
• Support compliance with applicable laws and regulations
• Promote responsible information handling practices
• Reduce information security risks
• Define information security responsibilities
• Support business continuity and operational resilience
• Establish minimum data protection requirements

2. SCOPE

This Policy applies to:
• All Employees
• Directors and Senior Management
• Contractors
• Consultants
• Temporary personnel
• Business Partners
• Third Parties who access, process or store information on behalf of GoldTakas FZCO

This Policy applies to:
• Electronic information
• Physical records
• Personal Data
• Confidential Information
• Company systems
• Devices
• Communication platforms
• Information assets owned, processed or controlled by GoldTakas FZCO

3. REFERENCE FRAMEWORK

This Policy has been prepared with reference to:
• Applicable UAE laws and regulations
• UAE Personal Data Protection Law (PDPL)
• DMCC requirements
• Information security best practices
• GoldTakas FZCO AML/CFT Policy

- GoldTakas FZCO Client Acceptance Policy
- GoldTakas FZCO Code of Ethics and Business Conduct Policy
- GoldTakas FZCO Whistleblowing Policy
- Other applicable internal policies and procedures

4. DEFINITIONS

Confidential Information: Any non-public information relating to GoldTakas FZCO, its Clients, Employees, suppliers or Business Partners.
Personal Data: Any information relating to an identified or identifiable natural person.
Information Asset: Any information, system, device, database, document or record owned, controlled or processed by GoldTakas FZCO.
Data Subject: An individual to whom Personal Data relates.
Information Security Incident: Any event that compromises, or may compromise, the confidentiality, integrity or availability of information.
Access Control: Measures designed to restrict access to authorized individuals.
Data Breach: Unauthorized access, disclosure, loss, destruction, alteration or misuse of Personal Data.
Processing: Any operation performed on Personal Data including collection, storage, use, transmission or deletion.

5. GOVERNANCE AND RESPONSIBILITIES

5.1 Senior Management

Senior Management is responsible for:
- Approving this Policy
- Supporting information security and data protection initiatives
- Ensuring adequate resources are available
- Reviewing significant information security incidents where appropriate

5.2 Compliance Function

The Compliance Function is responsible for:
- Monitoring compliance with this Policy
- Supporting incident reporting and escalation
- Coordinating awareness and training activities
- Monitoring regulatory developments
- Maintaining relevant records

5.3 Employees

Employees are responsible for:
- Protecting information assets
- Following security procedures
- Reporting security incidents promptly
- Maintaining confidentiality
- Using Company systems responsibly

5.4 Third Parties

Third Parties with access to information assets are expected to:

- Protect information appropriately
- Comply with contractual security obligations
- Report security incidents promptly
- Cooperate with security reviews where appropriate

6. INFORMATION SECURITY PRINCIPLES

GoldTakas FZCO applies information security controls designed to protect:

- Confidentiality
- Integrity
- Availability

of information assets.

Information shall be accessed, used, disclosed and stored only for legitimate business purposes.

Access shall be granted based on business need and authorized responsibilities.

Employees shall:

- Protect passwords and access credentials
- Prevent unauthorized access
- Secure physical and electronic records
- Use Company systems responsibly
- Follow applicable information security procedures

7. CONFIDENTIAL INFORMATION

Employees shall protect Confidential Information obtained through employment or business relationships.

Confidential Information shall not be:

- Shared with unauthorized individuals
- Used for personal benefit
- Disclosed without authorization
- Discussed in inappropriate environments

Confidentiality obligations continue after termination of employment or business relationships.

8. PERSONAL DATA PROTECTION

GoldTakas FZCO shall process Personal Data lawfully, fairly and responsibly.

Personal Data shall be:

- Collected for legitimate purposes
- Limited to what is necessary
- Accurate where reasonably practicable

• Protected against unauthorized access
• Retained only as long as necessary

Access to Personal Data shall be restricted to individuals with a legitimate business need.

9. ACCESS MANAGEMENT

Access to information assets shall be granted according to business responsibilities.

GoldTakas FZCO shall apply reasonable controls to:
• Create user accounts
• Modify access rights
• Remove access rights
• Review access permissions periodically

Access shall be revoked promptly when no longer required.

10. INFORMATION SECURITY INCIDENTS

Employees shall promptly report actual or suspected information security incidents.

Examples include:
• Unauthorized access
• Data breaches
• Lost or stolen devices
• Malware infections
• Phishing attempts
• Accidental disclosure of information
• Unauthorized system activity

Reported incidents shall be assessed, documented and addressed appropriately.

Actual or suspected information security incidents shall be reported promptly through the designated Compliance reporting channel at compliance.ae@goldtakas.com or through other incident reporting mechanisms designated by GoldTakas FZCO.

11. THIRD-PARTY INFORMATION SECURITY

Where Third Parties access, process or store information on behalf of GoldTakas FZCO, reasonable measures shall be taken to assess and manage associated risks.

Controls may include:
• Due diligence
• Contractual obligations
• Confidentiality requirements
• Access restrictions
• Monitoring activities

Third-Party access shall be limited to what is necessary for legitimate business purposes.

12. RECORD RETENTION AND DISPOSAL

GoldTakas FZCO shall maintain records in accordance with legal, regulatory and business requirements.

Records shall be:
• Protected against unauthorized access
• Retained for required periods
• Disposed of securely when no longer required

Personal Data and Confidential Information shall be destroyed or deleted in a secure manner when retention is no longer required.

13. TRAINING AND AWARENESS

GoldTakas FZCO shall provide information security and data protection training appropriate to employee responsibilities.

Training may cover:
• Information security principles
• Confidentiality obligations
• Data protection requirements
• Password security
• Phishing awareness
• Incident reporting
• Acceptable use requirements

Training shall be provided:
• Upon joining
• At least annually
• Following significant policy or regulatory changes
• Where additional training is necessary

Training records shall be documented and retained.

14. RECORD KEEPING

GoldTakas FZCO shall maintain records relating to:
• Information security incidents
• Data breaches
• Access reviews
• Training activities
• Security assessments
• Corrective actions
• Compliance reviews

Records shall be retained for a minimum of five (5) years or longer where required by applicable laws, regulations, investigations, audits or legal holds.

15. MONITORING AND REVIEW

The Compliance Function shall periodically review the effectiveness of information security and data protection controls.

Reviews may include:
• Security assessments
• Incident analysis
• Access reviews
• Compliance testing
• Audit findings
• Corrective action monitoring

This Policy shall be reviewed at least annually and whenever significant regulatory, operational or technological changes occur.

16. BREACHES AND DISCIPLINARY MEASURES

Failure to comply with this Policy may result in:
• Disciplinary action
• Suspension of access privileges
• Contractual action
• Termination of employment or business relationships
• Regulatory reporting where required
• Legal action where appropriate

Serious breaches involving Confidential Information, Personal Data or Company systems shall be treated with particular seriousness.

17. FINAL PROVISIONS

This Policy shall enter into force upon approval by Senior Management and shall remain effective until amended, replaced or withdrawn.

The Compliance Function shall be responsible for the interpretation, implementation and ongoing administration of this Policy.

All Employees, Business Partners and Third Parties are expected to comply with this Policy and support GoldTakas FZCO's commitment to information security, data protection, confidentiality and responsible information management.

In cases of uncertainty regarding the application or interpretation of this Policy, guidance shall be sought from the Compliance Function before any action is taken.