



CONFIDENTIALITY POLICY

นโยบายการรักษาความลับ

QRS Global - Confidentiality Policy

Table of Contents

A. Purpose and Scope	2
1. Purpose	3
2. Scope	3
3. Applicability	3
B. Definitions	3
1. Confidential Information	3
2. Personal Data	3
3. Business Information	3
C. Policy Principles	3
1. Confidentiality Commitment	3
2. Use of Information	3
3. Access Control	3
D. Data Sharing and Disclosure	3
1. Authorized Sharing	3
2. Legal and Regulatory Disclosures	3
3. Third-Party Agreements	3
E. Data Protection Measures	4
1. Encryption	4
2. Data Retention	4
3. Employee Training	4
F. Breach Management	4
1. Breach Detection and Reporting	4
2. Disciplinary Actions	4
3. Client Notification	4
G. Client Rights	4
1. Access and Correction	4
2. Consent Withdrawal	4
3. Complaints	4
H. Policy Review and Updates	4
1. Regular Review	4
2. Compliance Updates	4
3. Communication of Changes	4



A. Purpose and Scope

1. Purpose

This policy establishes the framework for protecting the confidentiality of sensitive information handled by QRS Global LLC, ensuring trust, compliance, and data integrity.

2. Scope

Applies to all employees, contractors, clients, and third parties interacting with QRS Global's services and systems.

3. Applicability

Covers all forms of confidential data including electronic, paper-based, and verbal information.

B. Definitions

1. Confidential Information

Information not publicly available, including client personal and financial data, business plans, and internal operations.

2. Personal Data

Any information relating to an identified or identifiable individual.

3. Business Information

Includes proprietary methods, trading strategies, software, and internal reports.

C. Policy Principles

1. Confidentiality Commitment

QRS Global commits to safeguarding all confidential information entrusted to it.

2. Use of Information

Data is used solely for intended business purposes, regulatory compliance, and client service improvement.

3. Access Control

Access is granted strictly on a need-to-know basis with appropriate security protocols.

D. Data Sharing and Disclosure

1. Authorized Sharing

Information is shared only with authorized parties under strict confidentiality agreements.

2. Legal and Regulatory Disclosures

Disclosure required by law or regulation will be handled responsibly and transparently.

3. Third-Party Agreements

Third parties accessing confidential information must comply with QRS Global confidentiality standards.

E. Data Protection Measures

1. Encryption

Confidential data is encrypted in transit and at rest.

2. Data Retention

Data retention follows legal requirements and business needs, with secure disposal thereafter.

3. Employee Training

Regular training is conducted on confidentiality and data protection.

F. Breach Management

1. Breach Detection and Reporting

Potential breaches are identified, investigated, and reported promptly.

2. Disciplinary Actions

Violations may lead to sanctions including termination.

3. Client Notification

Clients affected by breaches will be informed as per applicable laws.

G. Client Rights

1. Access and Correction

Clients may access and request correction of their data.

2. Consent Withdrawal

Clients can withdraw consent for data processing where applicable.

3. Complaints

Mechanisms exist for clients to report concerns regarding data handling.

H. Policy Review and Updates

1. Regular Review

The policy is reviewed periodically to ensure effectiveness.

2. Compliance Updates

Adjustments are made to comply with changing regulations.

3. Communication of Changes

Significant changes will be communicated to all stakeholders.