ISO 9001 Documentation
Confidentiality of Data

1. Purpose

The purpose of this document is to define the requirements for ensuring the confidentiality of data within the organization's Quality Management System (QMS) in accordance with ISO 9001:2015. This ensures that all quality-related data, information, and records — including customer information, product data, process records, audit results, and proprietary information — are protected from unauthorized access, disclosure, alteration, or destruction, thereby maintaining data integrity, security, and trust in support of quality objectives and regulatory compliance.

While ISO 9001 does not prescribe a standalone confidentiality policy, the protection of data confidentiality is essential to ensuring competence, consistency, and secure operations, and is therefore an integral part of operational control (Clause 8.5.1), risk management (Clause 6.1), and record control (Clause 7.5.3 / 8.5.1) under the QMS.

2. Scope

This procedure applies to:

All data and information related to the quality management system, including:

- Customer data (e.g., contracts, feedback, complaints, personal information)
- Product and service data (e.g., designs, specifications, test results)
- Process and operational data (e.g., procedures, work instructions, internal reports)
- Quality records (e.g., inspection records, audit reports, nonconformity logs)
- Supplier and partner information
- Employee data relevant to quality or operations
- Intellectual property and proprietary information

All forms of data, including:

- Paper-based documents
- Electronic files, databases, and systems

- Emails, shared drives, cloud storage, and collaboration platforms
- Verbal or visual information shared in meetings or secure zones
- All personnel, including employees, contractors, consultants, suppliers, and third parties who create, access, process, store, or transmit quality-related data on behalf of the organization

3. References

- ISO 9001:2015 – Quality management systems – Requirements (Clauses: 4.1, 4.2, 5.1, 5.2, 7.5, 8.5.1, 8.6, 9.1.3, 10.2)
- ISO/IEC 27001:2022 – Information Security Management Systems (for additional guidance, if applicable)
- ISO 27701:2019 – Privacy Information Management (if personal data is involved, optional but recommended)
- Organization's Quality Manual
- Document Control Procedure
- Record Control Procedure
- Information Security Policy
- Data Protection and Privacy Policy
- Access Control Procedure
- Risk Management Procedure
- Non-Disclosure Agreement (NDA) Templates\

4. Definitions

Term	Definition
Confidential Data	Information that is not publicly available and is protected due to its sensitivity, value, or legal requirements. Includes customer, employee, product, and proprietary information.
Data Confidentiality	The principle that ensures sensitive information is accessible only to authorized individuals and is protected against unauthorized access, use, or disclosure.
Data Owner	The individual or department responsible for determining the classification, access, and usage rules for specific data.
Data Custodian	The person or system responsible for the safe storage, backup, and protection of data in accordance with defined policies.
Authorized Access	Access to data that is granted based on role, need-to-know, and approved permissions.
Data Breach	Any unauthorized access, use, disclosure, alteration, or destruction of confidential data.

5. Confidentiality of Data Policy Statement

At EastRising, we recognize that the confidentiality of data is essential to maintaining customer trust, operational integrity, regulatory compliance, and the effectiveness of our Quality Management System. This policy establishes the principles and controls for protecting all quality-related and sensitive information from unauthorized access, use, disclosure, or loss. We are committed to:

❖ Protecting Confidential Information

Ensuring that all data related to customers, products, processes, employees, and the organization is protected against unauthorized access or disclosure.

❖ Classifying Data Appropriately

Identifying and classifying data based on its sensitivity and applying appropriate levels of protection.

❖ Controlling Access

Granting access to confidential data only to authorized personnel based on their role, responsibility, and business need.

❖ Secure Handling & Storage

Ensuring that all data — whether in paper or electronic form — is securely created, transmitted, stored, and disposed of.

❖ Using Approved Systems & Tools

Utilizing only authorized IT systems, cloud platforms, email, and communication tools for handling quality and confidential data.

❖ Training & Awareness

Educating employees and stakeholders on their responsibilities for data confidentiality and security.

❖ Responding to Incidents

Investigating and responding promptly to any suspected or actual data breach or confidentiality incident.

❖ Complying with Laws & Regulations

Ensuring that all data handling practices comply with applicable data protection, privacy, and confidentiality laws.

6. Policy Development and Approval

The Confidentiality of Data Policy shall be:

- ❖ Developed with input from IT, Quality Assurance, Information Security , Legal, HR, and Management
- ❖ Aligned with the organization's quality objectives, customer requirements, and regulatory obligations
- ❖ Reviewed for consistency with risk-based thinking (Clause 6.1) and the protection of sensitive quality information
- ❖ Approved by Top Management to ensure leadership commitment and organizational alignment

7. Data Classification and Control

Data Type	Examples	Protection Level	Controls
Highly Confidential	Customer contracts, personal data, trade secrets, audit reports	Restricted	Access limited to authorized individuals; encryption; strict logging
Confidential	Product designs, test results, internal reports, supplier data	Controlled	Access by role; password protection; secure storage
Internal Use Only	General procedures, meeting minutes, non-sensitive records	Limited	No external sharing; controlled distribution
Public	Marketing materials, published specifications	Open	No specific restriction

8. Key Controls for Data Confidentiality

8.1 Access Control

- Access to confidential data is granted on a need-to-know basis
- User access rights are managed via role-based permissions
- Password policies, multi-factor authentication, and user account management are enforced

8.2 Data Storage & Transmission

- Confidential data is stored in secure locations (physical or digital)
- Electronic data is protected via encryption, secure servers, and access logs
- Data transmission (e.g., email, file sharing) uses secure and approved methods

8.3 Document & Record Control

- Confidential records are controlled under the Document and Record Control Procedure
- Access to quality records is restricted and logged
- Retention and disposal follow defined retention schedules

8.4 Third-Party & Supplier Confidentiality

- Suppliers and contractors sign Non-Disclosure Agreements (NDAs)
- Data shared with third parties is protected via contracts and access controls

8.5 Physical Security

- Paper records are stored in locked cabinets or secure rooms
- Access to data centers, server rooms, and archives is restricted and monitored

9. Training and Awareness

- Employees receive confidentiality and data security training during onboarding and regularly thereafter

Training includes:

- Recognizing confidential information

- Proper handling and storage
- Reporting suspected breaches
- Using approved communication and storage tools

10. Monitoring, Auditing, and Incident Response

- Regular audits are conducted to ensure compliance with confidentiality controls
- Access logs and data usage are monitored for unusual activity
- Suspected breaches are reported immediately to the Data Protection Officer, IT, or Quality Manager

Incident response procedures include:

- Investigation
- Containment
- Notification (if required)
- Remediation and lessons learned

11. Management Review and Continuous Improvement

- The effectiveness of data confidentiality controls is reviewed as part of management review (Clause 9.3)
- Trends in incidents, audit findings, or employee feedback are used to drive continuous improvement
- The policy is updated as needed to reflect new risks, technologies, or regulatory changes

12. Compliance with ISO 9001:2015

This Confidentiality of Data Policy supports compliance with the following clauses of ISO 9001:2015:

Clause	Requirement Addressed
4.1	Understanding the organization and its context (including data-related risks)
4.2	Understanding the needs and expectations of interested parties (e.g., customers, regulators)
5.1	Leadership and commitment (demonstrating protection of critical data)
5.2	Quality Policy (aligning with ethical and secure information practices)

Clause	Requirement Addressed
6.1	Actions to address risks and opportunities (e.g., data breach risks)
7.5	Documented Information (protection of quality records and data)
8.5.1	Control of production and service provision (secure handling of operational data)
9.1.3	Monitoring, measurement, analysis and evaluation (data security performance)
10.2	Nonconformity and corrective action (addressing data breaches or mishandling)

13. Conclusion

Confidentiality of Data is a critical component of a robust Quality Management System. By protecting sensitive information related to products, customers, processes, and operations, the organization ensures data security, regulatory compliance, customer trust, and operational integrity.

This policy, when integrated with access controls, training, monitoring, and incident response, helps prevent data breaches, supports quality excellence, and reinforces the organization's commitment to ethical, secure, and responsible business practices — fully aligned with the principles of ISO 9001:2015.

14. Revision History of This Document

Rev No.	Date	Revised By	Approved By	Description
v1.0	2025-10-28	John Wang	Janice Lee	Initial release of ISO 9001 Documentation -Confidentiality of Data

Note: All controlled documents must be accessed through authenticated and approved channels. Employees must notify QA/Document Control in case they identify outdated or conflicting versions.

End of Document