ISO 9001 Documentation

Data Backups

1. Purpose

The purpose of this document is to define the requirements and procedures for implementing effective Data Backup practices within the organization's Quality Management System (QMS) in accordance with ISO 9001:2015. This ensures that all quality-related data and information, including electronic documents, records, test results, product data, customer information, and configuration settings, are regularly backed up, securely stored, and available for recovery in the event of data loss, system failure, disaster, or unintended deletion.

Data backups are a critical control to support data integrity, business continuity, and compliance with quality and regulatory requirements.

2. Scope

This procedure applies to:

- ❖ All data generated, processed, or maintained as part of the Quality Management System, including but not limited to:
- ✧ Quality records (e.g., inspection reports, audit records, nonconformity logs)
- ✧ Product and process data (e.g., specifications, test results, BOMs, drawings)
- ✧ Customer-related data (e.g., contracts, feedback, complaints)
- ✧ Documented information (e.g., procedures, work instructions, forms)
- ✧ Configuration data, software settings, and system parameters
- ✧ Electronic files stored on servers, local computers, cloud platforms, or shared drives

- ❖ All systems and media used to create, modify, store, or transmit quality-related data, including:
- ✧ Servers, databases, network drives
- ✧ Cloud storage and backup services
- ✧ Local PCs, laptops, and mobile devices (where quality data is stored)
- ✧ Backup hardware, software, and archival systems

- ✧ It covers the planning, execution, verification, storage, retention, and recovery of data backups across all departments and functions.

3. References

- ❖ ISO 9001:2015 – Quality management systems – Requirements (Clauses: 7.5, 8.5.1, 9.1.3, 10.2)
- ❖ Organization's Quality Manual
- ❖ Document Control Procedure
- ❖ Record Control Procedure
- ❖ IT Systems and Data Management Policy
- ❖ Risk Management Procedure (for data loss and business continuity risks)
- ❖ Business Continuity and Disaster Recovery Plan
- ❖ Information Security Policy

4. Definitions

Term	Definition
Data Backup	The process of creating and storing copies of electronic data to enable recovery in case of loss, corruption, or accidental deletion.
Backup Media	Physical or digital storage used to retain backup copies (e.g., external hard drives, tapes, cloud storage).
Backup Frequency	How often backups are performed (e.g., daily, weekly, real-time).
Retention Period	The defined length of time that backup data is retained before being archived or deleted.
Restore	The process of recovering data from a backup copy to restore it to its original or alternative location.
Disaster Recovery	The overall process of restoring IT systems and data following a major failure or disaster.

5. Data Backup Policy Statement

At EastRising , we recognize that data is a critical asset in the operation of our Quality Management System and in delivering consistent, high-quality products and services. This Data Backup Policy establishes the requirements for the regular, secure, and reliable backup of all quality-related data to prevent loss, ensure availability, and support business continuity.
We are committed to:

- ❖ Protecting Quality Data

Ensuring that all quality-related electronic data is backed up regularly to prevent loss due to system failure, human error, or disaster.

❖ Defining Backup Procedures

Establishing clear procedures for backup frequency, storage, retention, and restoration.

❖ Ensuring Data Integrity and Security

Protecting backup data from unauthorized access, corruption, or loss using secure methods and controlled access.

❖ Testing Backup and Restore Processes

Regularly verifying that backup data can be successfully restored to ensure reliability and readiness.

❖ Retaining Backups as Required

Storing backups for defined periods in line with legal, regulatory, and operational needs.

❖ Supporting Business Continuity

Ensuring that data backups are part of our broader disaster recovery and business continuity strategy.

6. Policy Development and Approval

The Data Backup Policy shall be:

- ❖ Developed with input from IT, Quality Assurance, Operations, and Management
- ❖ Aligned with the organization's quality objectives, risk management strategy, and compliance requirements
- ❖ Reviewed for consistency with Clause 7.5 (Documented Information) and Clause 8.5.1 (Control of Production and Service Provision) of ISO 9001:2015
- ❖ Approved by Top Management or IT Governance Authority to ensure organizational commitment

7. Backup Requirements and Controls

7.1 Data Identification

Identify all critical quality-related data that must be backed up, including:

- Quality records
- Product and process documentation
- Customer and supplier data
- Configuration and system files
- Audit and inspection data

7.2 Backup Frequency

Backup frequency is determined based on:

- Criticality of the data
- Rate of data change
- Regulatory or business requirements
- Typical frequencies include:
- Real-time / Continuous (for critical systems)
- Daily (for transactional or frequently updated data)
- Weekly or Monthly (for less dynamic records)

7.3 Backup Methods

Full Backups: Complete copy of all selected data

Incremental Backups: Only changes since the last backup

Differential Backups: Changes since the last full backup

Backups may be performed automatically (via software) or manually (for specific files or systems)

7.4 Backup Storage

Backup data is stored on:

- Secure internal servers
- Encrypted external drives
- Cloud-based backup solutions (with strong access controls)
- Backup media is stored in secure, access-controlled, and environmentally protected locations

- Offsite or cloud backups are used to protect against site-wide disasters

7.5 Retention Period

- Backup data is retained for a defined period based on:
- Regulatory requirements
- Customer or contractual obligations
- Operational or audit needs
- Typical retention:3 months to 7 years, depending on data type

7.6 Backup Security

- Backup data is encrypted during transfer and storage
- Access to backup systems and media is restricted to authorized personnel only
- Backup logs and activities are monitored and auditable

8. Backup Procedures

8.1 Performing Backups

- Backups are performed according to the defined schedule and method
- Automated backup jobs are monitored for success or failure
- Manual backups (e.g., for special projects) are documented and verified

8.2 Backup Verification

Regular checks are performed to confirm that:

- Backups are completing successfully
- Backup files are not corrupted
- Data can be restored (through periodic testing)

8.3 Restore Procedures

Restore processes are tested periodically

In case of data loss or system failure:

- Authorized personnel initiate the restore process
- Restored data is verified for accuracy and completeness

- Affected systems are brought back online following validation

9. Monitoring, Auditing, and Incident Response

- Backup logs are reviewed regularly for errors or failures
- Failed or missed backups are investigated and resolved promptly
- Data loss incidents are reported and managed under the Nonconformity and Corrective Action Procedure
- Audits may be conducted to verify compliance with backup policies

10. Training and Awareness

IT and key personnel are trained on:

- Backup procedures and schedules
- Secure handling of backup media
- Restore processes and emergency response

Employees are made aware of:

- The importance of data backups
- Proper saving and storage of quality-related files

11. Management Review and Continuous Improvement

- The effectiveness of the data backup process is reviewed as part of management review (Clause 9.3)
- Lessons learned from restoration incidents, audits, or near-misses are used to improve the process

Backup policies and technologies are updated to reflect:

- New risks
- Regulatory changes
- Technological advancements

12. Compliance with ISO 9001:2015

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

Clause	Requirement Addressed
7.5	Documented Information (ensuring protection and availability of quality records)
8.5.1	Control of Production and Service Provision (ensuring data integrity in operations)
9.1.3	Monitoring, Measurement, Analysis and Evaluation (monitoring backup performance)
10.2	Nonconformity and Corrective Action (addressing backup failures or data loss)

13. Conclusion

Data backups are a fundamental control within the Quality Management System to ensure the availability, integrity, and security of quality-related information. By implementing structured, secure, and regularly tested backup procedures, the organization protects itself from data loss, supports regulatory compliance, and ensures the continuity of quality operations.

This policy, combined with proper controls, verification, and recovery practices, enables the organization to maintain trusted, resilient, and high-quality processes in alignment with ISO 9001:2015 and best practices in information management.

14. Revision History of This Document

Rev No.	Date	Revised By	Approved By	Description
v1.0	2025-10-29	John Wang	Janice Lee	Initial release of ISO 9001 Documentation -Data Backups

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