



Data Management Policy

July 09, 2019

PUBLICATION NOTE	2
DOCUMENT MANAGEMENT	2
DOCUMENT APPROVAL AND ACCEPTANCE	2
1. PURPOSE	3
2. SCOPE	3
3. POLICY	3
1. DATA CLASSIFICATION	3
1.1 CONFIDENTIAL	3
1.2 RESTRICTED	3
1.3 PUBLIC	3
2. LABELING	4
2.1 CONFIDENTIAL	4
2.2 RESTRICTED	4
2.3 PUBLIC	4
3. HANDLING	4
3.1 CONFIDENTIAL	5
3.2 RESTRICTED	5
3.3 PUBLIC	5
4. DATA RETENTION	5
5. DATA & DEVICE DISPOSAL	5
6. ANNUAL DATA REVIEW	6
7. LEGAL REQUIREMENTS	6
4. AMENDMENT/TERMINATION OF THIS POLICY	6
5. EXCEPTIONS	6
6. VIOLATIONS/ENFORCEMENT	6



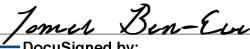
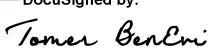
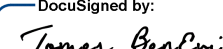
Publication Note

This policy is the property of Mursion and is exclusively for the use of Mursion employees, authorized agents, and affiliated companies. It contains Mursion confidential and proprietary information, and under no circumstances is it to be delivered or disclosed to any person not employed by Mursion, its authorized agents, or affiliated companies, without the express written authorization of an officer of Mursion.

Document Management

Revision	Release Date	Updated by	Remarks/Comments
0.1	5/6/19	M. Cooper	Initial Draft
0.2	5/17/2019	T.Ben-Evi	Second draft
1.0	6/10/2019	T Ben-Evi	SOC2 Ready

Document Approval and Acceptance

Name	Signature	Date
Tomer Ben-Evi		6/12/2019
Tomer BenEvi	DocuSigned by:  A1112A21C6D546F...	7/14/2020
Tomer Ben-Evi	DocuSigned by:  A1112A21C6D546F...	7/26/2021



1. Purpose

To ensure that information is classified, protected and handled in accordance with its importance to the organization.

2. Scope

All data and information systems owned by Mursion used to store, process, or transmit data, to all external parties, including, but not limited to Mursion consultants and contractors, business partners, vendors, suppliers, outsource service providers, and other third-party entities with access to Mursion networks and system resources.

3. Policy

Mursion classifies data and information system in accordance with legal requirements, sensitivity, and business criticality in order to ensure that information is given the appropriate level of protection. Data owners are responsible for identifying any additional requirements for specific data or exceptions to standard handling requirements.

Information systems and applications shall be classified according to the highest classification of data that they store or process.

1. Data Classification

To help Mursion and its employees easily understand requirements associated with different kinds of information, the company has created three classes of data. All classes and handling are further defined in the Data Classification Matrix. The Classification Matrix is attached as Appendix A to this policy.

1.1 Confidential

Highly sensitive data requiring the highest levels of protection; access is restricted to specific employees or departments, and these records can only be shared with others after obtaining approval from the data owner, or a company executive. Customer data, personally identifiable information (PII), company financial and banking data, payroll information, strategic plans, risk assessment reports, technical vulnerability reports, authentication credentials, private keys, and source code, are examples of data that is typically classified as confidential.

1.2 Restricted

Mursion proprietary information requiring thorough protection; access is restricted to employees with a “need-to-know” based on business requirements. This data can only be distributed outside the company with approval from the data owner. This is default classification for all company data unless stated otherwise. Internal policies, contracts, and various internal reports are examples of data generally classified as restricted.

1.3 Public

Documents intended for public consumption which can be freely distributed outside Mursion. Marketing materials, product descriptions, release notes, and external facing policies are examples of public data



2. Labeling

Mursion shall maintain an Information Systems Classification Matrix (Classification Matrix) identifying the classification of Mursion data and the primary Mursion information systems and applications. The Systems Matrix is attached as Appendix B to this policy.

2.1 Confidential

- All “Confidential” data shall be marked as such:
 - o Special handling instructions must be provided
 - o Each page if loose sheets
 - o Front and back covers, and title page if bound

2.2 Restricted

- All “Restricted” data shall be marked as such:
 - o Special handling instructions must be provided
 - o Front and back covers, and title page if bound
- If transmitting outside the Organization
 - o Mark as restricted on each page, if loose sheets

2.3 Public

- No special protection or handling requirements are required for Mursion Public data.
- Business units are encouraged to label such data as “Public” to assist other Mursion staff in identifying records that can be freely distributed outside the company.

3. Handling

3.1 Confidential

Confidential data is subject to the following protection and handling requirements:

- Access for non-preapproved-roles requires documented approval from the data owner
- Access is restricted to specific employees, roles and/or departments
- Confidential systems shall not allow unauthenticated or anonymous access
- Confidential data shall be encrypted in transit over public networks
- Mobile device hard drives containing confidential data, including laptops, shall be encrypted
- Mobile devices storing or accessing confidential data shall be protected by a log-on password or passcode and shall be configured to lock the screen after fifteen (10) minutes of non-use
- Backups shall be encrypted
- Physical backup media shall be labeled “Confidential”
- Confidential data shall not be stored on removable media including USB drives, CD’s, or DVD’s
- Paper records shall be labeled “confidential” and securely stored and disposed



- Hard drives and mobile devices used to store confidential information must be securely wiped prior to disposal or physically destroyed
- Transfer of confidential data to people or entities outside the company shall only be done in accordance with a legal contract or arrangement, and the explicit written permission of management or the data owner

3.2 Restricted

Restricted data is subject to the following protection and handling requirements:

- Access is restricted to users with a need-to-know based on business requirements
- Restricted systems shall not allow unauthenticated or anonymous access
- Transfer of restricted data to people or entities outside the company or authorized users shall require management approval and shall only be done in accordance with a legal contract or arrangement, or the explicit written permission of the data owner
- Paper records shall be securely stored and disposed
- Hard drives and mobile devices used to store restricted information must be securely wiped prior to disposal or physically destroyed

3.3 Public

No special protection or handling controls are required for public data. Public data may be freely distributed. Business units are encouraged to label such data as “Public” to assist other Mursion staff in identifying records that can be freely distributed outside the company.

4. Data Retention

Mursion shall retain data as long as the company has a need for its use, or to meet regulatory or contractual requirements. Once data is no longer needed, it shall be securely disposed of or archived. Data owners, in consultation with legal counsel, may determine retention periods for their data. Retention periods shall be documented in the Information Systems Classification Matrix.

5. Data & Device Disposal

Data classified as restricted or confidential shall be securely deleted when no longer needed. Mursion shall assess the data and disposal practices of third-party vendors in accordance with the Third-Party Management Policy. Only third-parties who meet Mursion requirements for secure data disposal shall be used for store and process restricted or confidential data.

Mursion shall ensure that all restricted and confidential data is securely deleted from company devices prior to, or at the time of disposal.



6. Annual Data Review

Data owners, together with IT management, shall implement a process for annual review of data aging. Data shall be disposed of in accordance with the Information Security Program Audit section.

7. Legal Requirements

Under certain circumstances, Mursion may become subject to legal proceedings requiring retention of data associated with legal holds, lawsuits, or other matters as stipulated by Mursion legal counsel. Such records and information are exempt from any other requirements specified within this Data Management Policy and are to be retained in accordance with requirements identified by the Legal department. All such holds and special retention requirements are subject to annual review between the IT Department and legal counsel to evaluate continuing requirements and scope.

4. Amendment/Termination Of This Policy

Mursion reserves the right to modify, amend or terminate this policy at any time. This policy does not constitute a contract between the company and its employees, partners, agents and contractors.

5. Exceptions

Requests for an exception to this Policy must be submitted to authorized personnel for approval. All exception requests will be handled in accordance with the Information Security Exception Policy and Standard.

6. Violations/Enforcement

Any known violations of this policy should be reported to the company's IT department. Violations of this policy can result in immediate withdrawal or suspension of system and Network privileges and/or disciplinary action in accordance with company procedures. The Mursion may advise law enforcement agencies when a criminal offense may have been committed.