Mozart ltd Data Management Policy

1. Purpose

This Data Management Policy establishes guidelines and standards for the management of Mozart ltd's data assets, ensuring they are properly protected, stored, processed, and disposed of throughout their lifecycle. As a B2B software provider handling sensitive information including Personally Identifiable Information (PII) and financial data, Mozart ltd is committed to maintaining the highest standards of data security and compliance.

The policy aims to reduce risks associated with data breaches, ensure compliance with relevant regulations including GDPR, and establish clear protocols for data management across our hybrid work environment. This document serves as a comprehensive framework to guide all employees in their daily handling of company and client data, with special consideration for our finance sector clients who require enhanced security measures.

2. Scope

This Data Management Policy applies to all employees, contractors, consultants, temporary staff, and other workers at Mozart ltd, including personnel affiliated with third parties who access Mozart ltd's network or data. It encompasses all data created, received, stored, or transmitted through Mozart ltd's systems, whether in digital or physical format, regardless of whether employees are working on-site or remotely in our hybrid work environment.

3. Policy

Mozart ltd requires all personnel to adhere to the data management practices outlined in this document to safeguard the integrity, confidentiality, and availability of company and client data. All employees must familiarize themselves with this policy and participate in regular training on data protection practices. Department managers are responsible for ensuring their teams comply with this policy, with oversight from the IT department and executive leadership.

4. Data Classification

Mozart ltd categorizes all data into three classifications based on sensitivity, regulatory requirements, and business impact if disclosed. All employees must understand these classifications to ensure appropriate handling and protection measures are applied consistently across our hybrid work environment.

4.1 Confidential

Confidential data is the most sensitive information that requires the highest level of protection. Unauthorized disclosure, alteration, or destruction of this data could cause significant damage to Mozart ltd, its clients, or employees.

Confidential data includes, but is not limited to:

- Personal identifiable information (PII) as defined by GDPR
- Financial records of clients, especially those in the finance sector
- Authentication credentials (passwords, security tokens)
- Mozart ltd's financial data and forecasts
- Source code for proprietary software products
- Client contracts and agreements
- Detailed security architecture information

4.2 Restricted

Restricted data is information that is not generally available to the public but has less stringent requirements than confidential data. While disclosure may not cause serious harm, it could negatively impact Mozart ltd's operations or reputation.
Restricted data includes, but is not limited to:

- Internal communications not intended for public distribution
- Product development roadmaps
- Non-sensitive client information
- Employee work information (email addresses, job titles, business phone numbers)
- Internal policies and procedures
- Meeting minutes and internal reports
- Non-confidential business strategies and plans

4.3 Public

Public data is information that has been approved for release to the general public and poses minimal risk to Mozart ltd if disclosed.
Public data includes, but is not limited to:

- Marketing materials and press releases
- Product descriptions and specifications available on the website
- Job postings
- Public-facing aspects of Mozart ltd's website
- Published white papers and case studies
- Social media content
- Information in the public domain

4.4 Labeling

All documents, files, and communications containing confidential or restricted data must be clearly labeled with their classification level. Digital files should include the classification in the filename, document header, or metadata where possible. Email subjects containing confidential information should be prefixed with [CONFIDENTIAL]. Physical documents must be labeled at the top and bottom of each page. When data classification is unclear, employees should default to treating information as restricted until proper classification is determined.

5. Data Handling

5.1 Confidential Data Handling

Confidential data requires the highest level of protection against unauthorized access or disclosure. Access must be strictly limited to individuals with a clear business need.
Requirements for confidential data:

- Must be encrypted at rest and in transit using industry-standard encryption protocols
- Access requires multi-factor authentication
- Must not be stored on personal devices under any circumstances
- Must not be shared via email without encryption
- Physical documents must be stored in locked cabinets when not in use
- Must not be discussed in public places or over unsecured communication channels
- When working remotely, confidential data must only be accessed through secure VPN connections
- Special handling procedures apply for finance sector clients' data, including enhanced logging and access controls
- Must be backed up according to the schedule in Appendix B

5.2 Restricted Data Handling

Restricted data requires protection from unauthorized access but may be shared more widely within Mozart ltd than confidential data.
Requirements for restricted data:

- Must be encrypted when transmitted outside the company network
- Access limited to authenticated users with appropriate permissions
- May be stored on company-approved devices with appropriate security controls
- Should not be printed unless necessary, and printed copies must be securely stored
- Remote access must be through secure connections
- Sharing with third parties requires a confidentiality agreement
- Must not be posted on public forums or social media
- Should be backed up according to the schedule in Appendix B

5.3 Public Data Handling

Public data has minimal security requirements as it is intended for public consumption.
Requirements for public data:

- May be freely disseminated without internal approval
- Should be reviewed for accuracy before publication
- Must not contain any confidential or restricted information
- Should be clearly identifiable as Mozart ltd content where appropriate
- Publishing new public data requires approval from the Marketing or Communications department
- Should be periodically reviewed to ensure continued relevance
- Must comply with Mozart ltd's branding guidelines

6. Data Retention

Mozart ltd retains data according to its classification, legal requirements, business needs, and contractual obligations. All data has a defined lifecycle, from creation through archiving to eventual deletion or destruction. Employees must adhere to the retention periods specified in Appendix B - Data Retention Matrix, which details the retention periods for different types of data based on classification and regulatory requirements including GDPR.

7. Data & Device Disposal

When data reaches the end of its retention period, it must be securely disposed of to prevent unauthorized access. Digital data must be permanently deleted using secure deletion methods that prevent recovery. This includes using specialized software to overwrite data multiple times on rewritable media, and degaussing or physically destroying non-rewritable media.
Hardware and devices containing data must be properly sanitized before reuse, recycling, or disposal. This includes computers, servers, mobile devices, USB drives, external hard drives, and any other storage media. IT department approval is required before disposing of any company device, and a record of all disposed devices and the method of data destruction must be maintained. For detailed procedures, refer to Appendix A - Internal Retention and Disposal Procedure.

8. Annual Data Review

Mozart ltd will conduct an annual data review to ensure compliance with this policy and to identify opportunities for improvement. Department heads are responsible for reviewing the data stored by their teams to verify proper classification, remove unnecessary data, and ensure compliance with retention policies. This review will include an audit of access controls to verify that they align with current business needs and that former employees no longer have access to company systems. The results of this review will be documented and presented to executive leadership along with recommendations for policy updates or process improvements.

9. Legal Requirements

Mozart ltd must comply with all applicable laws and regulations regarding data protection, including but not limited to the General Data Protection Regulation (GDPR). This includes maintaining appropriate technical and organizational measures to protect personal data, respecting data subject rights, conducting data protection impact assessments when required, and reporting data breaches to relevant authorities within required timeframes. Mozart ltd must also comply with any specific regulatory requirements applicable to our finance sector clients, which may include additional security measures and restrictions on data processing.

10. Policy Compliance

All employees, contractors, and third parties accessing Mozart ltd's systems or data are expected to comply with this Data Management Policy. Compliance will be verified through regular audits and monitoring of access logs, with results reported to executive leadership.

11. Exceptions

Any exceptions to this policy must be approved in writing by the Chief Information Officer or designated security officer. All exceptions must be documented, including the reason for the exception, the duration, and any compensating controls implemented to mitigate risks.

12. Violations & Enforcement

Violations of this Data Management Policy may result in disciplinary action, up to and including termination of employment or contract. The severity of the disciplinary action will depend on the nature and context of the violation, including whether it was intentional or accidental, and the potential impact on Mozart ltd, its clients, or employees. Any employee who becomes aware of a violation of this policy is required to report it to their manager, the IT department, or through Mozart ltd's anonymous reporting channel.

APPENDIX A - Internal Retention and Disposal Procedure

A.1 Data Identification

1. Department managers must identify and categorize data within their area of responsibility
2. Document the types of data, classification, location, and applicable retention requirements
3. Update the inventory annually or when significant changes occur

A.2 Retention Procedure

1. Store data according to its classification and the retention schedule
2. Implement appropriate access controls based on data classification
3. Maintain an audit trail of access to confidential and restricted data
4. Review data access permissions quarterly
5. Archive data that has exceeded its active period but is still within retention requirements

A.3 Disposal Procedure

1. Identify data that has reached the end of its retention period
2. Obtain approval from the department manager before disposal
3. For digital data:
    - Use secure deletion software that meets industry standards
    - Document the date and method of deletion
    - For cloud services, ensure data is purged from all backups
4. For physical documents:
    - Use cross-cut shredders for standard documents
    - Use certified destruction services for highly confidential materials
    - Obtain certificate of destruction when using external services
5. For electronic media:
    - Wipe all storage devices using approved methods
    - Physically destroy media that cannot be reliably wiped
    - Document the destruction method and date

6. Update data inventory to reflect disposal actions

APPENDIX B - Data Retention Matrix

Data Type	Classification	Retention Period	Disposal Method	Special Requirements
Customer PII	Confidential	Duration of service + 2 years	Secure deletion	GDPR compliance required
Employee records	Confidential	Duration of employment + 5 years	Secure deletion	Legal hold exceptions may apply
Financial transactions	Confidential	7 years	Secure deletion	Additional retention for finance clients
Contracts	Confidential	Duration of contract + 6 years	Secure deletion	Legal approval for early disposal
Product source code	Confidential	Perpetual for current versions; 5 years for deprecated versions	Secure deletion	Archive copy may be retained longer
Internal communications	Restricted	2 years	Standard deletion	Extend if relevant to active projects
System logs	Restricted	1 year	Standard deletion	Security incidents require extended retention
Marketing materials	Public	3 years	Standard deletion	Archive for historical reference
Client-specific customizations	Confidential	Duration of client relationship + 3 years	Secure deletion	Finance clients: retain for 7 years
Backups	Varies by content	Daily backups: 30 days; Weekly backups: 3 months; Monthly backups: 1 year	Secure deletion	Finance client data may require longer retention
Authentication logs	Confidential	1 year	Secure deletion	Extended retention for security investigations
Development documentation	Restricted	Duration of product life + 2 years	Standard deletion	Archive for reference
Public-facing website content	Public	Duration of publication + 1 year	Standard deletion	Archive copies for legal purposes