Harris McCall
CSIA 300
Matt Boehnke
Lab 2

XYZ Corp

Data Retention and Data Destruction Policy

Effective Date: 06/01/2023

1. Introduction

XYZ Corp (referred to as "the Company" from this point onward) recognizes the importance of managing and retaining data in a responsible and compliant manner. This Data Retention and Data Destruction Policy outlines the procedures and guidelines for the retention and secure disposal of company data.

2. Key Terms

1. **Data Classification:** The categorization of data based on its sensitivity, importance, regulatory requirements used to determine how to appropriately handle said data.
2. **Data Custodian:** The individual(s) responsible for overseeing the handling of data within the organization.
3. **Data Privacy Officer:** The individual who ensures compliance with data protection laws, regulations, and company policy.
4. **Secure Erasure:** The process of permanently and effectively deleting or disposing of data so that it is irrecoverable by any entity.
5. **Litigation Exception:** The act of preserving data for the use in pending or anticipated legal processes.

3. Purpose

The purpose of this policy is to:

1. Ensure that data is retained for the necessary amount of time required to meet legal, regulatory, and business requirements.
2. Minimize the risk of unauthorized access, use, or exposure of sensitive information.
3. Encourage efficient data management to reduce storage costs.

4. Define procedures for the secure erasure of data when it reaches the end of its retention period.

4. Scope

This policy applies to all employees, contractors, and third parties who have authorization to view, use, or manage any data owned or controlled by the company.

5. Data Classification

Data is classified into the following categories for the purpose of retention and disposal:

Critical Data	Data that is essential for business operations, regulatory compliance, or legal purposes.
Sensitive Data	Data that contains confidential, proprietary, or personally identifiable information.
Non-Essential Data	Data that is not critical for business operations, regulatory compliance, or legal purposes.

6. Retention Periods

Data may be kept longer than is listed on a case-by-case basis, as reviewed by the appointed Data Privacy Officer. The retention periods for each data category are as follows:

Critical Data	Retained indefinitely or as long as required by applicable laws and regulations.
Sensitive Data	Retained for a minimum period of 4 years, after which it may be securely disposed of.
Non-Essential Data	Retained for a minimum period of 6 months, after which it may be securely disposed of.

7. Data Disposal

Data disposal must be carried out in a secure and timely manner to prevent unauthorized access or disclosure. The following methods are approved for data disposal:

1. **Physical Media:** Must be shredded, pulped, or incinerated in accordance with state and federal laws.

2. **Electronic Media:** Secure erasure of data using approved software tools and techniques. Storage mediums must be properly degaussed or pulverized upon decommission.

8. Data Destruction Procedures

1. **Identification:** Data Custodians are responsible for identifying data that has reached the end of its retention period.
2. **Approval:** Data destruction requests must be approved by the Data Privacy Officer.
3. **Secure Disposal:** Data must be destroyed using the approved methods mentioned in Section 7.
4. **Documentation:** All data destruction activities must be documented, including the type of data destroyed, method and date of destruction, and the individuals responsible for the disposal of the data.

9. Litigation Exception Process

In the event of pending or anticipated litigation, data that may be relevant to the legal matter must be preserved and not subjected to routine data destruction. The process for litigation exception is as follows:

1. **Identification:** Upon notification of pending or anticipated litigation, the Legal Department, in consultation with the Data Custodian, will identify and specify the data to be preserved.
2. **Preservation:** The identified data must be preserved in its current state and not altered or destroyed until further notice from the Legal Department.
3. **Documentation:** All preservation activities must be documented, including the reason for preservation, the data involved, and the individuals responsible for preservation.

10. Legal and Regulatory Compliance

The Company is committed to complying with all applicable data protection laws and regulations at the State and Federal levels. The Company will retain data as long as is required by law and will cooperate with regulatory and/or legal authorities when necessary.

11. Data Access and Retrieval

During the data retention period, authorized personnel may access and retrieve data as needed for business purposes. All requests for data retrieval must be documented and approved by the Data Custodian or Data Privacy Officer.

12. Monitoring and Enforcement

The Company will periodically review and audit compliance with this Data Retention and Data Destruction Policy. Non-compliance may result in disciplinary or legal actions, up to and including termination of employment or contractual relationships.

13. Review and Revision

This Data Retention and Data Destruction Policy will be reviewed periodically and updated as necessary to reflect changes in laws, regulations, and business needs.

14. Contact Information

For questions or concerns related to this policy, please contact the Data Privacy Officer at:

Jane Westcliffe
j.westcliffe@xyz.org
(321)-135-9753

15. Acknowledgment

I acknowledge that I have received, read, and understood The Company's Data Retention and Data Destruction Policy. I agree to comply with its provisions and requirements.

Employee/Contractor Name: _____

Signature: _____

Date: _____

References

IRS. (2021). *Starting a Business and Keeping Records.* Washington D.C.: Internal Revenue Service. Retrieved from https://www.irs.gov/pub/irs-pdf/p583.pdf

NFIB. (2005). *Guide to Document Retention.* National Federation of Independent Business. Retrieved from https://www.nfib.com/documents/pdf/faststart/guide-to-doc-retention.pdf

Wrozek, B. (2001). *Electronic Data Retention Policy.* SANS. Retrieved from https://www.sans.org/white-papers/514/