Introduction: This Data Retention Policy outlines how an organization will retain and manage the data it collects, processes, and stores. Data retention policies are essential for managing data privacy and security risks, ensuring compliance with regulatory requirements, and preserving data for future use.

Scope: This policy applies to all data collected and processed by the organization and its employees, contractors, and third-party service providers.

Policy:

1. Purpose of Data Retention: The purpose of data retention is to ensure that data is retained for a specific period of time for legal, regulatory, operational, or historical purposes. The data retention policy should ensure that data is not retained beyond the necessary period.
2. Classification of Data: All data should be classified according to the sensitivity, confidentiality, and criticality of the data. The classification of data should be determined based on the impact on the organization if the data is lost, stolen, or compromised.
3. Retention Period: The retention period for data should be based on legal, regulatory, or business requirements. The retention period for different types of data should be reviewed periodically, and changes should be made as required.
4. Data Destruction: Data should be destroyed securely when it is no longer needed for the intended purpose or when the retention period expires. Data destruction should be performed in compliance with applicable laws, regulations, and industry standards.
5. Exceptions: Exceptions to this policy may be made on a case-by-case basis with the approval of the data owner or data custodian. Exceptions should be documented and justified.
6. Review and Update: This policy should be reviewed and updated periodically to ensure compliance with legal and regulatory requirements and changes in business practices.
7. Responsibility: The responsibility for implementing this policy and ensuring compliance with the policy lies with the data owner or data custodian.

Conclusion: This Data Retention Policy is an essential part of an organization's data management strategy. It provides a framework for managing data retention, ensuring compliance with regulatory requirements, and protecting sensitive data from unauthorized access, use, or disclosure. The organization should ensure that all employees, contractors, and third-party service providers are aware of this policy and are trained on its requirements.