Data Retention and Deletion Policy

Purpose

This policy outlines the requirements and procedures [ORG] has implemented to manage the retention and deletion of data. The objective is to ensure data is retained only for as long as necessary to meet legal, regulatory, and operational requirements and to minimize risks associated with over-retention of data, including potential cyberattacks and legal subpoenas.

Scope

This policy applies to all staff and personnel across the [ORG]. All staff members interact with organizational data to varying extents, depending on their roles and responsibilities. The relevance of specific elements of this policy may vary based on individual roles and levels of responsibility for handling, retaining, and deleting data. All staff are expected to familiarize themselves with the details of this policy and adhere to its guidelines when managing data.

Designated personnel responsible for ensuring compliance with this policy are tasked with securely archiving or deleting data at the end of its retention period, as outlined in the Data Retention and Deletion Schedule. Adherence to this policy is essential for maintaining the security and integrity of organizational data.

This policy applies to all information handled by the organization, including but not limited to data received, stored, processed, or transmitted in any form. This includes electronic data, physical documents, and other media, regardless of the format or storage method.

Roles and Responsibilities

Data Lead

The Data Lead is responsible for:

- Monitoring applicable state, national, and international laws related to data privacy and implementing processes to ensure compliance.
- Consulting with legal counsel regarding changes to data privacy laws and their impact on the organization's data practices.
- Reviewing contracts with vendors, especially those involving tools or systems that process sensitive data, to ensure compliance with privacy standards and protection of individualized data.
- Evaluating reported or discovered data breaches or incidents and escalating them for confidential investigation by the appropriate team or committee.

Data Governance Team (DGT)

The Data Governance Team is responsible for:

- Identifying areas where data classification, handling, or retention practices require improvement.
- Contributing to the development and implementation of policies, processes, and tools to enhance data management across the organization.

Department and Program Heads

Department and program leaders are responsible for:

- Ensuring their team members have appropriate training and resources to securely handle data in line with their job responsibilities.
- Supporting compliance with organizational policies by promoting a culture of data security and awareness.

Employees and Contractors

Employees and contractors who handle sensitive data must:

- Follow all organizational policies related to data confidentiality, including any specific confidentiality and list-sharing policies.
- Review and acknowledge this policy annually as part of their commitment to safeguarding data.

All Staff and Partners

All employees, contractors, board members, and partners with access to organizational data are responsible for:

- Adhering to this policy and ensuring that sensitive and confidential information is always protected.
- Acting with integrity and diligence when handling data and reporting any concerns or incidents to the appropriate point of contact.

Policy

[ORG] is committed to managing data responsibly and in compliance with applicable laws and regulations. Data will be retained for specified periods based on the type of data and its relevance to the organization's operations. Upon reaching the end of the retention period, data will be securely deleted or archived as per the guidelines outlined in this policy. All stakeholders will be informed of the data retention and deletion policies and their rights to request data deletion. Requests for data deletion will be evaluated and processed in accordance with this policy. Where required and appropriate, it is essential to indicate where consent has been collected for the retention and processing of data.

Data Retention and Deletion Schedule

Category	Data Element	Storage System	Retention Time	Retention/ Deletion	Consent Required?
Development	Donor Personal Identifying Information	CRM System, Cloud Storage	10 years	Archive	Yes
Development	Donations and Donor Transactions	Financial System, CRM System	7 years	Archive	Yes
Development	Supporter Records and Campaign Engagement	CRM System, Cloud Storage	5 years	Deletion	Yes
Communication Records	Correspondence, Email, and Chat (General)	Email/Chat Systems	1 year	Deletion	No
Communication Records	Press Releases and Public Documents	Website, Cloud Storage	5 years	Archive	No
Communication Records	Non-Program Related SharePoint and Teams Sites	Cloud Collaboration Tools	1 year	Deletion	No
Governance	Minutes of Board and Board Committee Meetings	Shared Drive, Secure Folder	Permanent	Archive	No
Governance	Board Policies/Resolutions	Shared Drive, Secure Folder	Permanent	Archive	No
Programs	Program Records	Shared Drive, Local Server	5 years	Deletion	No
Programs	Material of Historical Value	Archives, Shared Drive	Permanent	Archive	No

Classification:

Restricted	
Confidential	
Internal	
Public	

Secure Deletion Methods

[ORG] is committed to securely deleting data when it's no longer needed, or its retention period expires. This section outlines approved methods for secure deletion of digital and physical data.

Digital Data Deletion

1. **Software-based Deletion**: Use certified data erasure software that overwrites data multiple times.
2. **Physical Destruction**: For decommissioned devices:
    - HDDs: Degaussing or shredding
    - SSDs and portable media: Physical shredding or pulverizing
3. **Cloud-based Data**: Use secure deletion features provided by the cloud service provider.

Physical Document Destruction

1. Use cross-cut shredders or professional shredding services.
2. For highly sensitive documents, consider pulping or incineration at certified facilities.

Best Practices

1. Maintain a log of all deletion activities.
2. Regularly train staff and volunteers on secure deletion procedures.
3. Ensure third-party service providers comply with these deletion standards.

By following these methods, [ORG] aims to minimize unauthorized access risks and protect stakeholder privacy and security.

Ongoing Review

[ORG] will review and update this policy at least annually to ensure its continued effectiveness and alignment with data collected best practices and legal requirements.

Revision History

Version	Date	Editor	Description of Changes
1.0	[Date]	[Editor]	Initial Creation
1.1			