Introduction

Organisation seeks to ensure that it retains only data necessary to effectively conduct its program activities and work in fulfilment of its mission. The need to retain data varies widely with the type of data and the purpose for which it was collected. Organisation strives to ensure that data is only retained for the period necessary to fulfil the purpose for which it was collected and is fully deleted when no longer required. This policy sets forth Organisation's guidelines on data retention and is to be consistently applied throughout the organization.

Scope

This policy covers all data collected by Organisation and stored, owned or leased systems and media, regardless of location. It applies to both data collected and held electronically (including photographs, video and audio recordings) and data that is collected and held as hard copy or paper files. The need to retain certain information may be mandated by federal or local law, federal regulations and legitimate business purposes.

Reasons for Data Retention

Cloud data retention is the practice of storing, archiving, or otherwise retaining data in cloud storage.

There are three types of cloud data storage that may be used to facilitate cloud data retention:

1 **Object Storage** - Object storage designates each piece of data as an object, adds comprehensive metadata to every object, and eliminates the hierarchical organization of "files and folders". Data in object storage is placed into a flat address space called a storage pool, a practice which results in faster data retrieval and more efficient analytics.

2 **File Storage** - In a file storage system, data exists in named files that are organized into folders. Folders may be nested in other folders, forming a hierarchy of data-containing directories and sub-directories. Files may have limited metadata associated with them, such as the file name, date of creation, and the date it was last modified.

3 **Block Storage** - Block storage technology separates data into blocks, breaks those blocks into separate pieces, assigns each piece a unique identifier code, and stores the data on a Storage Area Network (SAN). SANs present block storage to other networked systems, leveraging a high-speed architecture to deliver low-latency data access and facilitate high-performance workloads.

The amount of data enterprise businesses capture and produce can be staggering:

- **Customer data:** Customer lists, contracts, invoices, purchase orders, tax ID numbers, credit card numbers/tokens
- **Financial data:** Balance sheets, tax records, expenses
- **Human resources data:** Payroll, employee records, workers' compensation claims, performance evaluations
- **Company communications:** Emails, text messages, attachments, enterprise platform chats
- **Operational information:** Quality control reports, audits, test results, proposals, board meeting records, certifications
- **Proprietary data:** Management information, new project data, executive communications, intellectual property, business assets, other key records.

An effective records retention policy must cover all of these records and many others. Enterprise archives can easily involve hundreds of terabytes of data or more.

Guiding Data Retention Principles

Guiding data retention principles are:

Fairness: All Processing of Personal Data must be fair, proportionate and compatible with the purposes for which the data were collected.

Necessity: Personal Data are deleted when no longer needed.

Security: Personal Data are protected by appropriate security measures.

It needs to be ensured that each principle set out at paragraph above is followed whenever a Processing activity is envisaged or planned for or on behalf of organisation.

Data Duplication

Organisation seeks to avoid duplication in data storage whenever possible, though there may be instances in which for programmatic or other business reasons it is necessary for data to be held in more than one place. This policy applies to all data in Organisation's possession, including duplicate copies of data.

Retention Requirements

Organisation has set the following guidelines for retaining all personal data as defined in the Institute's data privacy policy.

• Website visitor data will be retained as long as necessary to provide the service requested/initiated through the Organisation website.

• Contributor data will be retained for the year in which the individual has contributed and then for [Duration] after the date of the last contribution. Financial information will not be retained longer than is necessary to process a single transaction.

• Event participant data will be retained for the period of the event, including any follow up activities, such as the distribution of reports, plus a period of [Duration];

• Program participant data (including sign in sheets) will be retained for the duration of the grant agreement that financed the program plus any additional time required under the terms of the grant agreement.

• Personal data of subgrantees, subcontractors and vendors will be kept for the duration of the contract or agreement.

• Employee data will be held for the duration of employment and then [Duration] after the last day of employment.

• Data associated with employee wages, leave and pension shall be held for the period of employment plus [Duration], with the exception of pension eligibility and retirement beneficiary data which shall be kept for [Duration].

• Recruitment data, including interview notes of unsuccessful applicants, will be held for [Duration] after the closing of the position recruitment process.

• Consultant (both paid and pro bono) data will be held for the duration of the consulting contract plus [Duration] after the end of the consultancy.

• Board member data will be held for the duration of service on the Board plus for [Duration] after the end of the member's term.

• Data associated with tax payments (including payroll, corporate and VAT) will be held for [Duration].

• Operational data related to program proposals, reporting and program management will be held for the period required by the Organisation donor, but not more than [Duration].

A solid data retention plan with secure backups can save your business if a ransomware attack blocks your access to key records.

Deletion Policy

At some point, you'll no longer need the data and want to cut costs on storage by deleting it. The deletion policy determines when you can discard the data without affecting compliance or business recovery.

Data Destruction

Data destruction ensures that Organisation manages the data it controls and processes it in an efficient and responsible manner. When the retention period for the data as outlined above expires, Organisation will actively destroy the data covered by this policy. If an individual believes that there exists a legitimate business reason why certain data should not be destroyed at the end of a retention period, he or she should identify this data to his/her supervisor and provide information as to why the data should not be destroyed. Any exceptions to this data retention policy must be approved by Organisation's data protection offer in consultation with legal counsel. In rare circumstances, a litigation hold may be issued by legal counsel prohibiting the destruction of certain documents. A litigation hold remains in effect until released by legal counsel and prohibits the destruction of data subject to the hold.

DISCIPLINARY

- Hillwood takes its data retention obligations seriously. Hillwood will, if required, report violations of this Policy and related provisions to relevant regulatory, governmental and other competent authorities.
- It is your responsibility to comply with this Policy. Failure to comply may leave you personally liable for civil or criminal penalties (including civil or criminal penalties and fines).
- Breaches of this Policy are recorded and monitored. Failure to comply maybe taken into account during performance reviews for Hillwood's employees, associates and service providers.