DATA ARCHIVING AND RETENTION POLICY

PURPOSE

In accordance with industry best practices and to comply with relevant compliance regulations, the provider has implemented a range of Information Security policies and procedures designed to protect the confidentiality, integrity, and availability (CIA) of critical client data, computing resources, and business interests.

This document describes the data archiving and retention policies and procedures to be performed by the provider IT department.

POLICY STATEMENT

GENERAL POLICY

Any data deemed a *business record* must be archived and retained for a specified period of time. A business record includes any print or electronic document created and maintained in the normal course of business. However, not all data qualifies as a business record that must be retained.

Data and any corresponding attachments should be retained if they document business activities that have evidentiary or reference value, or if they represent the sole copy of required information. Examples include job offers, contract negotiations where final pricing has been set, and policy memos.

Items that **do not** require retention include:

- In-progress drafts
- Internal discussions
- Negotiations without finalization
- Duplicate copies where an original exists
- Non-business correspondence

Any data required by law for legal reviews or audits must be archived and retained for the legally mandated duration. Disposal of such data must occur in accordance with applicable regulations governing the provider and the industry in which it operates.

MANAGEMENT RESPONSIBILITIES

Management is responsible for ensuring that procedures for archiving and retaining electronic data comply with all applicable local, state, federal, and industry laws, regulations, and directives. Management must remain aware of and maintain documentation relating to these legal and regulatory requirements, including any changes that may impact this Data Archiving and Retention Policy.

PROVIDER IT DEPARTMENT RESPONSIBILITIES

The provider IT department is responsible for implementing and supporting an appropriate data archiving solution and any required supporting software.

All archived data must be tagged with metadata to ensure that data headers, content, attachments, and text remain fully searchable. The provider IT department will also deploy and maintain software applications that support the storage, archiving, and search functionality of retained data.

DATA CLASSIFICATION

The following categories should be used to classify archived data. If data does not clearly fall within one of these categories, management and the provider IT department must assess it to determine appropriate retention guidelines.

Administrative Correspondence

Administrative Correspondence includes clarification of established company policy, such as holiday schedules, timekeeping information, dress code standards, workplace behavior expectations, and legal matters including intellectual property issues.
All communications containing this type of information that are sent to or from management should be classified as Administrative Correspondence.

Fiscal Correspondence

Fiscal Correspondence includes all information related to revenue, expenses, or financial reporting for the provider.

General Correspondence

General Correspondence includes information related to customer interactions and operational decision-making within the business.
Individual employees are responsible for the retention of their General Correspondence.

Ephemeral Correspondence

Ephemeral Correspondence is the largest category and includes personal messages, requests for reviews or recommendations, internal emails regarding product development, updates, and routine status reports.

Customer-Sensitive or Confidential Information

- Refer to the Information Security Policy for detailed classifications.
- Data must be destroyed upon completion of the related project, as agreed with customers.
- Data that becomes public due to age or lifecycle changes must be destroyed according to storage, backup, and computing resource requirements.

POLICY SUSPENSION

In accordance with industry best practices and compliance regulations, the provider has implemented Information Security policies and procedures to safeguard confidentiality, integrity, and availability of critical client data, computing resources, and business interests. This document outlines the necessary data archiving and retention procedures to be executed by the provider IT department.