Data Retention Policy

Kidd Insurances iss hereinafter referred to as "the company."

1.0 Overview

The need to retain data varies widely with the type of data. Some data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. Since this can be somewhat subjective, a retention policy is important to ensure that the company's guidelines on retention are consistently applied throughout the organisation.

2.0 Purpose

The purpose of this policy is to specify the company's guidelines for retaining different types of data.

3.0 Scope

The scope of this policy covers all company data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location.

Note that the need to retain certain information can be mandated by local, industry regulations and will comply with EU General Data Protection Regulation GDPR and the Data Protection Act 1988 and the Data Protection (Amendment) Act 2003. Where this policy differs from applicable regulations, the policy specified in the regulations will apply.

4.0 Policy

4.1 Reasons for Data Retention

The company does not wish to simply adopt a "save everything" approach. That is not practical or cost-effective and would place an excessive burden on company and IT Staff to manage the constantly-growing amount of data.

Some data, however, must be retained in order to protect the company's interests, preserve evidence, and generally conform to good business practices. Some reasons for data retention include:

- Litigation
- Accident investigation
- Security incident investigation
- Regulatory requirements
- Intellectual property preservation

4.2 Data Duplication

As data storage increases in size and decreases in cost, companies often err on the side of storing data in several places on the network. A common example of this is where a single file may be stored on a local user's machine, on a central file server, and again on a backup system. When identifying and classifying the company's data, it is important to also understand where that data may be stored, particularly for duplicate copies, so that this policy may be applied to all duplicates of the information.

4.3 Retention Requirements

This section sets guidelines for retaining the different types of company data.

- Personal customer data: Personal data will be held for as long as the individual is a customer of the company plus 6 years.
- Personal employee data: General employee data will be held for the duration of employment and then for 6 year after the last day of contractual employment. Employee contracts will be held for 6 years after last day of contractual employment.
- Tax payments will be held for six years.
- Records of leave will be held for three years.

- Recruitment details: Interview notes of unsuccessful applicants will be held for 1 year after interview. This personal data will then be destroyed.
- Planning data: 7 years.
- Health and Safety: 7 years for records of major accidents and dangerous occurrences.
- Public data: Public data will be retained for 3 years.
- Operational data: Most company data will fall in this category. Operational data will be retained for 5 years.
- Critical data including Tax and VAT: Critical data must be retained for 6 years.
- Confidential data: Confidential data must be retained for 7 years.

4.4 Retention of Encrypted Data

If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

4.5 Data Destruction

Data destruction is a critical component of a data retention policy. Data destruction ensures that the company will use data efficiently thereby making data management and data retrieval more cost effective. Exactly how certain data should be destroyed is covered in the Data Classification Policy.

When the retention timeframe expires, the company must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be a pp roved only by a member or members of the company's management team.

The company specifically directs users not to destroy data in violation of this policy. Destroying data that a user may feel is harmful to himself or herself is Particularly forbidden, or destroying data in an attempt to cover up a violation of law or company policy.

4.6 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Definitions

Backup: To copy data to a second location, solely for the purpose of safe keeping of that data.

Encryption: The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.

Encryption Key: An alphanumeric series of characters that enables data to be encrypted and decrypted.