Data Retention Policy

Introduction

Purpose

CIS Security Ltd is committed to being transparent about how it collects and uses the personal data and to meeting its data protection obligations. This policy sets out the organisation's commitment to data retention, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of all CIS stakeholders including job applicants, employees, workers, contractors, volunteers, interns, apprentices, former employees, clients, suppliers and future clients.

CIS Security Ltd has appointed Jon Felix as its Data Protection Officer. His role is to inform and advise the organisation on its data protection obligations. He can be contacted at dpo@cis-security.co.uk. Questions about this policy, or requests for further information, should be directed to the Data Protection Officer.

Definitions:

- "Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.
- "Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and genetic and biometric data.
- "Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

1. Scope

All Organisation Name's records, whether analogue or digital, are subject to the retention requirements of this policy

2. Responsibilities

2.1 The following roles are responsible for retention of these records because they are the information asset owners.

2.2 Asset owners are/responsible for ensuring that all personal data is collected, retained and destroyed in line with the requirements of the GDPR.

2.3 The Finance Director (FD) is responsible for retention of financial (accounting, tax) and related records.

2.4 The HR Director (HRD) is responsible for retention of all HR records.

2.5 The Health and Safety Manager (SHEQ) is responsible for retention of all Health and Safety records.

2.6 The Information Security Manager (ISM) is responsible for the retention of data within CIS IT systems.

2.7 The Data Protection Officer (DPO) is responsible for storage of data in line with this procedure.

2.8 The Managing Director (MD) is responsible for retention of all other statutory and regulatory records.

2.9 The Managing Director (MD) is responsible for ensuring that retained records are included in business continuity and disaster recovery plans.

3. Procedure

3.1 The required retention periods, by record type, are recorded in (Retention of Records Master Log on the company server under the following categories):

- 3.1.1 Record type
- 3.1.2 Retention period
- 3.1.3 Retention period to start from (at creation, submission, payment, etc.)
- 3.1.4 Retention justification
- 3.1.5 Record medium
- 3.1.6 Disposal method

Data Security

The organisation takes the security of personal data seriously. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. Access to the CIS internal IT infrastructure is controlled by password protection and as such has measures in place to minimise risk of illegal access from outside parties. All external third-party systems used by CIS are password protected and access is restricted in line with the role of employee.

All internal data used by CIS is backed up daily and held externally by a third party on servers located in the UK at a bomb-proof, flood-proof and EMP-proof data centre and holds both ISO27001 and ISO9001 certifications.

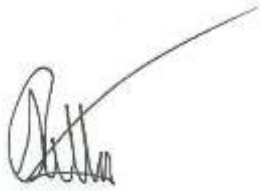
Data Retention Policy

Document Owner and Approval

The Managing Director is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements of the GDPR.

A current version of this document is available to all stakeholders on the website and internal members of staff on the employee portal and Y:\ drive. It does not contain confidential information and can be released to relevant external parties.

This information security policy was approved by the Board of Directors on 18/05/2018 and is issued on a version-controlled basis under the signature of CIS Managing Director.

Signature: 

Date: 18th May 2018

Change History Record

Ref	Issue	Description of Change	Approval	Date of Issue
IMSM.016	1	Initial issue	Managing Director	18.05.18