



PASSION. DETERMINATION. LEADERSHIP

Integrated Management System		Date	15/03/21
Title	Data Breach Policy	Issue	3
Ref	IMSM.013	Approved	N. Catton

Data Breach Policy

Introduction

The Board of Directors and management of CIS Security Ltd, located at CIS Security Ltd, 418-426 Lewisham High Street, London SE13 6LJ, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation in order to preserve its competitive edge, cashflow, profitability, legal, regulatory and contractual compliance and commercial image. Information and information security requirements will continue to be aligned with CIS Security Ltd's goals and the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations and for reducing information-related risks to acceptable levels.

CIS Security Ltd aims to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and the risk treatment plan.

All Employees/Staff of CIS Security Ltd and any third parties working on behalf of CIS Security Ltd are expected to comply with this policy and with the ISMS that implements this policy. All Employees/Staff, and certain external parties, will receive appropriate training. The consequences of breaching the information security policy are set out in the disciplinary policy and in contracts and agreements with third parties.

The ISMS is subject to continuous, systematic review and improvement.

CIS Security Ltd has established a top level management steering group (GDPR Strategy Group), chaired by the HR Director and including the Information Security Manager and other executives/specialists/risk specialists to support the ISMS framework and to periodically review the security policy.

CIS Security Ltd is committed to achieving certification of its ISMS to ISO27001:2013 and compliance with the GDPR.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

In this policy, 'information security' is defined as:



Preserve

This means that management, all full time or part time Employees/Staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches and to act in accordance with the availability. . .

the availability,

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient and CIS Security Ltd must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity and disaster recovery plans. Employees are only permitted to access the *CIS Security Ltd* network or company's email through devices issued by CIS Security Ltd that meet the agreed security standards and that are password protected. No employee is permitted to use any personal device such as mobile phone, tablet, laptop or PC to access or store any data relating to CIS Security Ltd as the security of these devices cannot be verified and therefore could present a security risk to the company.

confidentiality

This involves ensuring that information is only accessible to those authorised to access it and therefore to prevent both deliberate and accidental unauthorised access to CIS Security Ltd's information and proprietary knowledge and its systems including its network(s), website(s), extranet(s), and e-commerce systems.

and integrity

This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency including for network(s), e-commerce system(s), website(s), extranet(s) and data backup plans and security incident reporting. CIS Security Ltd must comply with all relevant data-related legislation in those jurisdictions within which it operates.

of the physical (assets)

The physical assets of CIS Security Ltd including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

and information assets.

The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context, 'data' also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc).

A SECURITY BREACH

Is any incident or activity that causes, or may cause, a break down in the availability, confidentiality or integrity of the physical or electronic information assets of CIS Security Ltd.

The Controller will notify CIS DPO (Data Protection Officer) dpo@cis-security.co.uk of any security breach within 24 hours (from the time of discovery of the breach) so that the DPO may notify the ICO (Information Commissioner's Office) within 72 hours from the discovery of the identified breach.

In the event that CIS Security is the processor in the relationship with a member of CIS Staff or Client it is the processor's duty to notify the controller of the data breach within 24 hours, be it a CIS employee or Client so that they may then follow the process described above.

CIS Data Protection Officer can be contacted here:

- dpo@cis-security.co.uk
- 020 8690 1903

Example of a reportable

Theft or loss of an unencrypted laptop computer or other unencrypted portable electronic/digital media holding names, addresses, dates of birth and National Insurance Numbers of 100 Individuals.

Example not reportable

Theft or loss of a marketing list of 100 names and addresses (or other contact details) where there is no particular sensitivity of the product being marketed

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 members of staff on the company website 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

Date Reviewed 15/03/21

Change History Record

Ref	Issue	Description of Change	Approval	Date of Issue
IMSM.013	1	Initial issue	Managing Director	18.05.18
IMSM.013	2	Review of document	Managing Director	23.03.20
IMSM.013	3	Review of document	Managing Director	15.03.21