Showpiece Design Limited, Tithe Barn Home Farm, Sulham Lane, Pangbourne, Berkshire, RG8 8DT

INFORMATION SECURITY POLICY

Our Board and management are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the Company in order to preserve its competitive performance, gain new business, increase profitability, comply with legal, regulatory and contractual compliance and enhance the Company's commercial image.

Information and information security requirements will continue to be aligned with the company's goals and this policy is intended to be an enabling mechanism for information sharing, for electronic operations and for reducing information-related risks to acceptable levels. The objective of the policy is to provide a secure business environment for the conduct of operations.

Our strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of a compliant Information Security Policy (ISP) and Information Security Management Systems (ISMS).

The Managing Director is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

Business continuity and contingency plans, data back-up procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy.

Control objectives for each of these areas are filed and are supported by specific, documented policies and procedures.

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

Preserving

This means that management, all full time or part time staff, subcontractors, 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 requirements
-

The consequences of security policy violations are described in the Company's disciplinary policy. All staff will receive information security awareness training and more specialized staff will receive appropriately specialized information security training.

The Availability

This means that information and associated assets should be accessible to authorized users when required and therefore physically secure. The computer network must be resilient and the Company must be able to 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 plans.

Confidentiality

This involves ensuring that information is only accessible to those authorized to access it and therefore to preventing both deliberate and accidental unauthorized access to the Company's information and its systems.

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 unauthorized modification, of either physical assets or electronic data.

There must be appropriate contingency and data back-up plans, and security incident reporting. The Company must comply with all relevant data-related legislation in those jurisdictions within which it operates.

Of Physical (Assets)

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

And Information (Assets)

The information assets includes:

- Information printed or written on paper;
- Information stored electronically on
- Servers;
- web site(s);
- PCs and laptops;
- CD ROMs;
- floppy disks;
- USB sticks;
- back up 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 the Organisation.

The Company Director is the Owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements in relation to ISO 9001 and ISO 27001.

A current version of this document is available to all members of staff. It does not contain confidential information and can be released to relevant external parties.

Signature: **Date:** **24th January 2017**

Name: **Deanne White** **Position:** **Director**

Version Control

Issue	Description	Change Date	Made By	Approved	Approval date
1.0	**Policy Statement**			**Yes**	**24/01/2017**
PRINTED COPIES WILL BE UNCONTROLLED					