Information Security *Policy*

vizst TECHNOLOGY

Version	Date Issued	Brief Summary of Change	Owner's Name
V1.0	19/03/18	New working document	Dan Warren
V2.0	08/10/21	Rebrand and updates	Dan Warren
V2.1	10/10/22	Minor Updates & Review	Dan Warren
V2.2	11/09/23	Minor Updates & Review	Dan Warren
V2.2	10/10/24	Annual Review	Dan Warren
V3.0	01/09/25	Review (template change)	Dan Warren

Introduction

This top-level information security policy is a key component of Vizst Technology's overall information security management framework and should be considered alongside more detailed information security documentation including, system level security policies, security guidance and protocols or procedures.

It is the expectation of Vizst Technology, its suppliers and contractors and anyone holding or processing any data on behalf of Vizst Technology, its staff, or customers, that all due care and consideration is demonstrated at all times, in order to safeguard that data to avoid data breech or loss. Vizst Technology will seek evidence that such safeguarding techniques are in place and are adhered to.

Objectives, Aim and Scope

Objectives

- The objectives of Vizst Technology's Information Security Policy are to preserve:
- Confidentiality - Access to Data shall be confined to those with appropriate authority.
- Integrity – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- Availability - Information shall be available and delivered to the right person, at the time when it is needed.

Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by Vizst Technology by:

- Ensuring that all members of staff, suppliers and contractors, are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principals of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

Scope

This policy applies to all information, information systems, networks, applications, locations and users of Vizst Technology or supplied under contract to it.

Responsibilities for Information Security

Ultimate responsibility for information security rests with the Chief Executive of Vizst Technology, but on a day-to-day basis the Operations Director shall be responsible for managing and implementing the policy and related procedures.

Line Directors are responsible for ensuring that their permanent and temporary staff and contractors are aware of:-

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

The Information Security Policy shall be maintained, reviewed and updated by the Operations Director. This review shall take place annually or as needed.

Line Directors shall be individually responsible for the security of their physical environments where information is processed or stored.

Each member of staff shall be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

Contracts with external contractors that allow access to the organisation's, or its customers', information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

Legislation

Vizst Technology is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the Vizst Technology, who may be held personally accountable for any breaches of information security for which they may be held responsible. The Vizst Technology shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (2018)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- General Data Protection Regulation (GDPR) (2018)
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000

- Freedom of Information Act 2000
- Health & Social Care Act 2001

Policy Framework

Management of Security

At board level, responsibility for Information Security shall reside with the Chief Executive Officer.

Vizst Technology's Senior Leadership Team shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.
- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.

Information security expectations of staff shall be included within appropriate job definitions.

Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

Computer Access Control

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the Operations Director.

Information Risk Assessment

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of Vizst Technology's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

Information security events and weaknesses

All information security events and suspected weaknesses are to be reported to the Operations Director. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

Classification of Sensitive Information.

A consistent system for the classification of information within Vizst Technology, enables common assurances in information partnerships, consistency in handling and retention practice when information is shared with non-Vizst Technology bodies.

Vizst Technology shall implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within the IG Toolkit to secure their information assets.

The classification Highly Confidential – shall be used for staff and customer records, personally identifiable information passing between Vizst Technology staff and between Vizst Technology staff and staff of other appropriate agencies. In order to safeguard confidentiality, the term "Highly Confidential" shall not be used on correspondence to a customer.

Documents so marked shall be held securely at all times within Vizst Technology's secure, online databases, to which only authorised persons have access. They shall not be available at any time, in any place, where unauthorised persons might gain access to them.

Documents marked Highly Confidential not in a safe location for any reason, should be kept out of sight of anyone not authorised to view them.

The classification Confidential - shall be used to mark all other sensitive information such as financial and contractual records. It shall cover information that the disclosure of which is likely to:

- adversely affect the reputation of the organisation or its officers, or cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness of the organisation;
- cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- breach statutory restrictions on disclosure of information;
- disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

Internal documents should also be stored within Vizst Technology's online secure databases and only available to those who have full justification to access them.

The classification Internal – shall be used to mark all documentation that is meant for the sole use of Vizst Technology staff or contractors, such as;

- policy information
- internal news items
- notices
- etc

Documents so marked shall be held securely at all times within Vizst Technology's secure, online databases, to which only authorised persons have access. They shall not be available at any time, in any place, where unauthorised persons might gain access to them.

Documents marked Vizst Technology Confidential not in a safe location for any reason, should be kept out of sight of anyone not authorised to view them

The classification Public – are documents intended for unrestricted public viewing, such as promotional material.

Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the treat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation's property without permission from the service desk. Users breaching this requirement may be subject to disciplinary action.

User media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of the service desk before they may be used on Vizst Technology systems. Such media must also be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action.

Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

Vizst Technology has in place routines to regularly audit compliance with this and other policies. In addition, it reserves the right monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human rights Act

Accreditation of Information Systems

The organisation shall ensure that all new information systems, applications and networks include a security plan and are approved by the Operations Director before they are put into a live environment.

System Change Control

Changes to information systems, applications or networks shall be subject to full change approval process and approved by the Operations Director or Chief Executive Officer.

Intellectual Property Rights

The organisation shall ensure that all information products are properly licensed and approved by the Operations Director. Users shall not install software on the organisation's property without permission from the Operations Director. Users breaching this requirement may be subject to disciplinary action.

Business Continuity and Disaster Recovery Plans

The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

Reporting

The Operations Director shall keep the Chief Executive Officer informed of the information security status of the organisation by means of regular reports and presentations as necessary.

Policy Audit

This policy shall be subject to audit as required.

Further Information

Further information and advice on this policy can be obtained from Dan Warren, Operations Director, 03333 442204.