Information Security Policy

TekTube Information Security Policy

Document Type: Policy

Version No: v1.0
Issue Date: 1st April 2018

Purpose of this document

To provide customers & suppliers with our Information Security Policy.

VERSION HISTORY

Version	Date Issued	Brief Summary of Change	Owner's Name
V.0	31/12/2017	Draft Policy	Neil Molton
V.1	1/4/2018	Approved and Implemented	Neil Molton

For more information on the status of this document, please contact:	Neil Molton Managing Director TekTube Ltd A5 Grovehill Industrial Estate Beck View Road Hull HU17 0GJ Tel: 0148 223 8030 E-mail: neil@TekTube.co.uk Internet: *www.tektube.co.uk/administration/infosecpolicy*
Date of Issue	1/4/2018
Reference	ISP.27001
© TekTube Ltd	

Policy title:	InfoSec Policy

Issue date:	1/4/2018	Review date:	1/4/2019

Version:	v1.0	Issued by:	Neil Molton

Aim:	Establish and maintain the security and confidentiality of information

Scope:	Applies to all information, information systems, networks, applications, locations and users of TekTube or supplied under contract to it.

Associated documentation:	**Legal Framework:** The Data Protection Act (1998) The Data Protection (Processing of Sensitive Personal Data) Order 2000. 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 European Union (EU) General Data Protection Regulation (GDPR) 2018 **Policies:** Acceptable Use Policy Backup Policy Incident Response Policy Virtual Private Network (VPN) Policy Wireless Policy Network Security Policy Confidential Data Policy Mobile Device Policy Outsourcing Policy Email Policy Password Policy Network Access Policy Remote Access Policy Guest Access Policy Third Party Connection Policy Encryption Policy Data Classification Policy Retention Policy Physical Security Policy
Appendices:	None
Approved by:	Neil Molton
Date:	1/4/2018

Review and consultation process:	Annually from review date above
Responsibility for Implementation & Training:	Neil Molton

HISTORY

Revisions:		
Date:	Author:	Description:
1/1/2018	NM	V.0 - Draft
1/4/2018	NM	V.1 - Approved

Distribution methods:	Soft copy - Email to all company employees Hard copy – Company Noticeboard

1. Introduction

This information security policy is a key component of our 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.

TekTube Ltd, Beverley, East Yorkshire (hereafter known as TekTube) recognise the importance of reliable information, both in terms of the management of staff and the efficient management of services and resources. TekTube also recognise the duty of confidentiality owed to staff, business partners and customers with regard to all the ways in which they process, store, share and dispose of information. Confidentiality and data protection legislation and guidance provide a framework for the management of all data from which individuals & companies can be identified. It is essential that all staff and contractors of TekTube are fully aware of their personal responsibilities for information which they may come into contact with.

2. Objectives, Aim and Scope

2.1. Objectives

The objectives of the TekTube 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.

2.2. 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 TekTube:

- Ensuring that all members of staff 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.

2.3. Scope

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

3. Responsibilities for Information Security

3.1. Ultimate responsibility for information security rests with the Managing Director of TekTube, as does the day-to-day responsibility for managing and implementing the policy and related procedures.

3.2. Line Managers 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

3.3. 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.

3.4. The Information Security Policy shall be maintained, reviewed and updated by the Managing Director. This review shall take place annually.

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

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

3.7. 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.

3.8. Contracts with external contractors that allow access to the organisation's 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.

4. Legislation

4.1. TekTube 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 TekTube, who may be held personally accountable for any breaches of information security for which they may be held responsible. TekTube shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- 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
- European Union (EU) General Data Protection Regulation (GDPR) 2018

5. Policy Framework

5.1. Management of Security

- At board level, responsibility for Information Security shall reside with the Managing Director.
- The TekTube Security Officer shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

5.2. 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.

5.3. 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.

5.4. Security Control of Assets

Each IT asset (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

5.5. 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.

5.6. User Access Controls

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

5.7. Computer Access Control

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

5.8. 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.

5.9. Equipment Security

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

5.10. Computer and Network Procedures

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

5.11. 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 TekTube'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.

5.12. Information security events and weaknesses

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

5.13. Classification of Sensitive Information.

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

TekTube shall implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within our processes to secure our information assets.

The classification **TekTube Confidential** – shall be used for customers' records, customer identifiable information passing between TekTube staff and between TekTube staff and staff of other appropriate agencies. In order to safeguard confidentiality, the term "TekTube Confidential" shall **not** be used on correspondence to a customer in accordance with the Confidentiality: TekTube Code of Practice. Documents so marked shall be held securely at all times in a locked cabinet to which only authorised persons have access. They shall not be left unattended at any time in any place where unauthorised persons might gain access to them. They should be transported securely. Documents marked TekTube Confidential not in a safe store or in transport should be kept out of sight of visitors or others not authorised to view them.

The classification **TekTube Restricted -** 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 it's 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.

TekTube Restricted documents should also be stored in lockable cabinets

5.14. Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the threat 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 Managing Director. Users breaching this requirement may be subject to disciplinary action.

5.15. 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 Managing Director before they may be used on TekTube 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.

5.16. 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.

TekTube 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

5.17. Accreditation of Information Systems

TekTube shall ensure that all new information systems, applications and networks include a security plan and are approved by the Managing Director before they commence operation.

Development of a series of System Level Security Policies (SLSPs) for systems under our control is in progress, in order to distinguish between the security management considerations of internal systems and that of subcontracted systems. In this way, specific responsibilities may be assigned and obligations communicated directly to those who use the system.

5.18. System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Managing Director.

5.19. Intellectual Property Rights

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

5.20. 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.

5.21. Reporting

The Information Security Officer shall keep records of the information security status of TekTube by means of continual assessment to company logs.

5.22. Policy Audit

This policy shall be subject to audit by the Managing Director.

5.23. Further Information

Further information and advice on this policy can be obtained from Joseph Moulin, TekTube Administration using 01482-238030 or joseph@tektube.co.uk.

6. Policy approved by:

Signature ____________________ Date 1st April 2018
Managing Director