TECHTRIO

BUILDING RELATIONSHIPS THROUGH TECHNOLOGY

INFORMATION SECURITY POLICY

1. Introduction

This policy underpins all TECHTRIO policies, procedures, standards and guidance for the security of electronically stored data.

In today's interconnected digital landscape, safeguarding sensitive information is paramount to our organisation's success and reputation. This policy outlines our commitment to maintaining the confidentiality, integrity, and availability of our information assets. By adhering to these guidelines, we ensure the protection of our data from unauthorised access, disclosure, alteration, or destruction.

This policy serves as a foundation for establishing a robust information security framework, guiding our employees, contractors, and stakeholders in their responsibilities towards safeguarding our valuable assets. We encourage everyone within our organisation to familiarise themselves with this policy and actively contribute to the culture of security awareness and compliance. Together, we uphold our commitment to protecting our information assets and maintaining the trust of our customers, partners, and stakeholders.

2. Scope

This policy applies to all information assets, including but not limited to data, systems, networks, applications, and physical assets, managed by TECHTRIO. It encompasses all employees, contractors, third-party vendors, and stakeholders who have access to or handle sensitive information on behalf of TECHTRIO.

3. Information Security Controls

The TECHTRIO Information Security Policy follows the principles, guidelines and responsibilities as set out in the Information Security Management System (ISMS) ISO 27001 ISO/IEC 27001:2022

These include:

- Data will be protected in line with relevant legislation, notably those relating to Data Protection, Human Rights and Freedom of Information as well as relevant TECHTRIO policies.
- Each information asset group will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset.
- Data will be made available solely to those who have a legitimate need for access.
- Sensitive data will be encrypted both at rest and in transit to protect it from unauthorised access or interception.
- It is the responsibility of all individuals who have been granted access to data to handle it appropriately in accordance with its classification.
- Regular Security Awareness Training will be provided to employees to educate them about information security best practices and their roles and responsibilities.
- Incident response procedures are in place to promptly detect, respond to, and recover from security incidents or breaches.
- Business continuity and disaster recovery plans are in place to ensure the uninterrupted availability of critical information resources.
- Data will be protected against unauthorised access.
- Compliance with the Information Security Policy will be enforced.

4. Roles & Responsibilities

All approved users of TECHTRIO's services must demonstrate an understanding of the Data Protection Act 2018. Staff must successfully complete the mandatory Information Security Awareness and Data Protection Training computer-based courses every two years.

Security responsibilities should be included in job role descriptions, person specifications and personal development plans. Individuals accessing TECHTRIO's data must seek advice from management if they are not clear about their information security responsibilities.

Employee contracts enforce compliance with TECHTRIO's policies.

Upon termination of a staff appointment, TECHTRIO will revise the staff record system, accordingly, triggering IT systems account termination processes. Not all system access is automatically controlled, for example local systems and records. Therefore, line managers must ensure that appropriate staff exit procedures are in place to remove access to all systems upon staff exit or change of role.

Line managers must ensure that all IT assets owned by TECHTRIO must be returned upon termination of contract.

The ISM may authorise legally compliant monitoring of IT systems to investigate security incidents and compliance with TECHTRIO's' policies.

5. Physical and environmental security

Computer equipment must be password protected if left unattended. A screen lock must be activated when there is no activity for a short period of time. Passwords must not be written down anywhere near IT equipment.

Portable computing devices must be locked away at the end of the working day.

All TECHTRIO owned equipment must be disposed of in a controlled manner. Any staff wishing to dispose of IT equipment must contact the TECHTRIO helpdesk to arrange collection.

6. Compliance

Compliance with the controls in this policy will be monitored by the ISM and reported to the ISSG.

The design, operation and use of IT systems must comply with all contracts and regulations, relevant UK, EU, and international law. This includes the Data Protection Act 2018, the Payment Card Industry Data Security Standard (PCI-DSS) where relevant and the UK Government's Prevent duty

TECHTRIO is subject to an independent audit and aims to comply with the spirit of ISO 27001 and the UK Governments Cyber Essentials scheme. Business critical systems and other systems identified as high risk will be regularly penetration tested.

7. Sanctions

Security incident investigation, or the failure to comply with this policy subsidiary policies, procedures or regulations, may result in withdrawal of access to TECHTRIO's IT services and may result in disciplinary action or termination of contract.

8. Exceptions

If an individual or third party cannot comply with this policy they must contact the TECHTRIO Helpdesk for advice on security controls to enable compliance, otherwise they must cease using TECHTRIO's data and IT services.

9. Policy Review and Updates

This Information Security Policy is reviewed annually or as necessary to ensure its continued effectiveness and relevance. Any updates or revisions to the policy will be communicated to all relevant stakeholders in a timely manner.

10. Definitions

- ISSG: Information Security Steering Group
- ISMS: Information Security Management System.
- ISO: International Standards Organisation
- ISO 27001: Industry standard for an ISMS
- GDPR: General Data Protection Regulation
- ISM: Information Security Manager
- DPO: Data Protection Officer

11. Conclusion

TECHTRIO is committed to maintaining the highest standards of information security to protect the confidentiality, integrity, and availability of our information assets. By adhering to this policy and working together towards our common objectives, we reinforce our commitment to excellence in information security management.

Authorised by:

Samad Choudhury

Director

01/01/2024