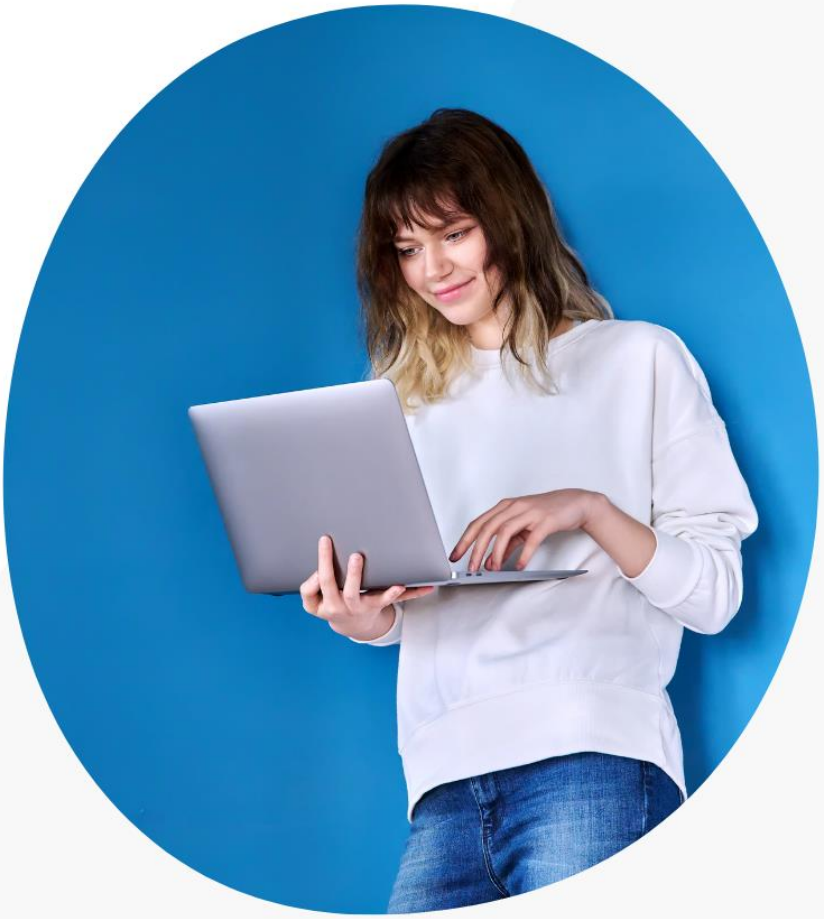
Information Security Policy

2024-25

Think Learning



Think Learning Policy
4th April 2024

1 Introduction

1.1 Background

This Information Security Policy is based upon the International Standard ISEC/ISO 27001 :2022 standard and guidelines.

think learning

CERTIFICATE OF REGISTRATION

ISO QUALITY SERVICES LTD.
BS EN ISO

This document certifies that the Management System of

Think Associates Ltd

1 Friary, Temple Quay, Bristol, Somerset, BS1 6EA

has been approved by

ISO Quality Services Limited

to the following Standard and Guidelines:

ISO 27001 : 2022

The approved Management System applies to the following:

HR Technologies Consulting Company delivering
Professional Services and Software

ISO QUALITY SERVICES LTD.
BS EN ISO

For and on behalf of
ISO Quality Services Limited

Director

Certificate No.	Originally Issued	Current Certificate	Certificate Expiry
QFOPB141801	11th March 2015	3rd April 2024	2nd April 2025

This certificate remains valid while the holder maintains their Management System in accordance with the Standard and Guidelines stated above which will be audited by ISO Quality Services Limited. This certificate remains the property of, and must be returned to, ISO Quality Services Limited on reasonable request.

Quality Suite, Oak House, Everoak Industrial Estate, Bromyard Road, Worcester, WR2 5HP, United Kingdom

This policy is also aligned to the UK Government back Cyber Essential scheme with the associated Cyber Liability Insurance, and also PCI DSS SAQ D version 3.2.1 for Service Providers dated 13th March 2024 (The Attestation of Compliance is available on request.)

1.2 Requirements for Policy

THINK ASSOCIATES LTD T/A THINK LEARNING (hereafter referred to as the Company) has an obligation to clearly define requirements for the use of its information technology (IT) facilities and its information systems (IS) to all staff, suppliers and partners.

The objective of this requirement is to ensure that users of IT/IS facilities do not unintentionally place themselves, or the Company, at risk of prosecution or disciplinary action, by carrying out computer related activities which contravene current policy or legislative restrictions.

Information within the Company is intended to be openly accessible and available to all members of the organisation for sharing and processing. Certain information (sensitive information) has to be processed, handled and managed securely and with accountability.

This policy outlines the control requirements for all information contained within the Company network and IT systems.

1.3 Policy Structure

This document forms the Company's Electronic Information Security Policy. Its purpose it to provide an overarching framework (a commitment of undertaking) to apply information security controls throughout the Company.

Supporting policies and guidance documents containing detailed Information security requirements will be developed in support of this policy. Dependent upon the subject matter, supporting policies and guidance will either apply across the Company or to more specific groups or individuals within the Company.

1.4 Purpose and Scope

All processing of data and collection of information will be processed in accordance with UK law. This policy defines how the Company will secure electronic information, which is found within:

- The Company's IS/IT infrastructure.
- Key Business System data and information.
- Security of information held in electronic form on any Company computer.

And is processed or used by:

1. Company Staff and suppliers who have access to or administer the Company network or IT systems.
2. External users, agents, and guest users authorised to use the Company network or IT Systems.
3. Individuals who process key data and information within Key Business Systems.

1.5 Objectives

These Information Security objectives are designed to protect Think Learning business information and client data within its custody or safekeeping by safeguarding its confidentiality, integrity and availability. In doing this the company will:

1. To provide systems that meet the requirements for the UK Government 'Official' **security classification** assessed through annual submission the G-Cloud and DOS procurement frameworks and the aligned NCSC Cloud Security Principles
2. Establish safeguards to protect all company and client information resources from theft, loss, abuse, misuse and any form of damage.
3. Establish responsibility and accountability for Information Security within the organisation.
4. Ensure that management and staff have an appropriate level of awareness, knowledge and skill to allow them to minimise the occurrence and severity of Information Security incidents.
5. Ensure that the organisation is able to continue its commercial activities in the event of significant Information Security incidents.
6. To provide suitable coverage of ISO27001:2022, Cyber Essentials plus and PCI DSS through ongoing audits.

Think Learning is committed to protecting its employees and Key Business Systems. Controls will therefore be deployed that mitigate the risk of vulnerabilities being exploited which adversely affect the efficient operation of the Company.

1.6 Applicability

This policy applies to all users of the Company network and IT Services and includes:

- All full-time, part-time and temporary staff employed by, or working for or on behalf of, the Company;
- Suppliers working at the Company;
- Third party contractors and consultants working for or on behalf of the Company;
- All other individuals and groups who have been granted access to the Company's network or IT Services.

These categories of persons and agencies are collectively known as the 'user' in the policy document.

The Directors of the Company are ultimately responsible for ensuring that adherence to this policy is observed and for overseeing compliance by users under their direction, control or supervision.

Each user is responsible for their own actions and must ensure all actions relating to using the Company network and IT Services adheres to the principles and requirements of this policy.

1.7 Legislation

Supply and use of the Company network and IT Services is bound by English law.

1.8 Associated Policies

The company handbook further defines individual responsibilities for data protection and information governance.

2 Information Security – Risk Management

Information security governance is the structure which supports the implementation of this policy. An IT infrastructure will be implemented within the Company to ensure the effective and efficient implementation of this policy across the Company.

2.1 Ownership and Maintenance of Policy

This policy is owned by the Company and is maintained, reviewed and amended by the Information Security Manager in accordance with Company policy, procedures and guidance.

This policy will be subject to review each year, as well as ad-hoc review if the Information Security Manager considers there to be a new or changed threat to respond to.

2.2 Risk Management and Electronic Service Incidents

The Company will be responsible for raising an incident message in relation to any reported security incident at the Company. These incidents will be recorded as 'Electronic Security Incidents'.

Electronic Security Incidents will be recorded with a unique reference number. A review of incidents will be conducted at six monthly intervals. Incidents considered to be exhibiting unacceptable levels of risk to the Company network or IT Services will be subject to an investigation to identify the inherent vulnerabilities exposed by this incident. A report will be submitted to the IT manager for consideration of the question of suitable remedial action which may be effectively implemented to mitigate future risks.

2.3 Security of Third Party Access

Procedures are in place to regulate access to the Company's information processing facilities by third parties. Such access will be controlled and regulated in order to protect information assets and prevent loss or damage to data through unauthorised access. The Information Security Manager will consider applications for access to facilities by contractors or third parties based upon a risk assessment of the proposed task.

2.4 Identification of Risk from Third Party Access

Third parties who require access to the Company's IT/IS infrastructure will be bound by contracts which define Company security requirements. Prior to being granted any connectivity to the Company's core internal or hosted systems, they will be required to sign and undertaking to adhere to the requirements of the Company policy and where sensitive information or sensitive business / research information is involved they will be required to sign a non-disclosure agreement prior to access.

3 Asset Clarification

Information assets are categorised and recorded to enable appropriate management and control.

3.1 Inventory of Assets

The Company maintains an inventory, subject to audit, of IR related assets.

For each item, the inventory will state the item's description, make, model, serial number and/or service tag and location. This inventory is in addition to asset records maintained under Company financial regulations. Specific systems and databases are also recorded in this inventory, along a role responsible for the system/database.

Any system and the data it contains that is not part of the above inventory is the responsibility of the creator of that system. However, the asset will require compliance with this policy and users will be required to adhere to the principles of this document.

All asset identification procedures must be compliant with and support the Company Business Continuity Plan.

4 Personnel Security Issues – Roles and Access Levels

The Company maintains a directory on Office 365, of people and suppliers which are authorised to use the Company network, IT services and applications. All users, staff, suppliers, external users and guest users are subject to the principles of this policy and must confirm that they agree to the terms.

If a user's relationship with the Company alters, due to a change in role or employment relationship, then the revised level of access must match both the new role and relationship with the Company. All IT account access levels must comply with the requirements of the Company policy.

4.1 Security in Job Descriptions

Security roles and responsibilities will be included in job descriptions and associated Company Handbooks where appropriate. These will include any specific responsibilities for the protection of particular assets, or the execution of particular processes or activities such as data protection.

4.2 Confidential Personal Data – Sensitive Information

All data which identifies any individual will be handled in accordance with the Data Protection Act 2018. All personal details will be held securely and in accordance with current applicable legislation.

All data classified as sensitive data will be processed and stored in compliance with the current sensitive information guidelines and Company policies and procedures.

4.3 Confidentiality Undertaking

All suppliers, members of staff and partners are reminded of their obligation to protect confidential information in accordance with the Company's standard terms and conditions of employment.

All users will be bound by the confidentiality agreement in either their contract or terms of employment.

4.4 Employee Responsibilities

All staff (including agency and casual staff) must agree to written terms and conditions contained within the Company handbook.

The Company shall ensure that:

- Confidentiality agreements form part of the terms and conditions of employment;
- Awareness training about electronic information security forms part of Company staff induction programmes with annual refresher training

- Information for all staff on electronic information security is maintained in the Company information;
- At least 2 references for a period extending to three years prior to the recruitment date are checked by personnel prior to a member of staff's commencement of employment.

The Company must ensure that where there are specific security roles and responsibilities they are documented in all relevant job descriptions and that there is appropriate screening of applicants.

4.5 Staff Leaving Employment

On termination of employment with the Company, any applicable user accounts, accesses and passwords will be changed or removed. Further information about procedures on termination of employment are contained in the Company handbook.

4.6 Responding to Security Incidents

4.6.1 Suspected Security Breach

The Information Security Manager will be responsible for identifying members of staff who are responsible for security breach investigations.

A security incident is any incident which alters, destroys or amends data within the Key Business Systems without authority. This may cause damage to or reduce the efficiency of the Company network or IT Services. This includes any actions or behaviours which contravenes Company policy, statutory or common law, legal requirements or professional regulation or guidance.

4.6.2 Reporting Security Incidents

All staff are made aware of the process to follow in the event of a serious security breach (for example lost or stolen devices). This process is defined below:

- Report to all directors (initial director will inform other directors)
- If you are reporting a stolen item, report this to the police
- If able, initiate a remote wipe of the device (if this is a company credit card report to the bank and cancel this card)

- Inform colleagues that you no longer have this device
- Director will judge whether to report this loss to clients, based on the risks
- Update the incident log and other relevant records

All suspected security incidents are to be reported immediately to all of the Company Directors.

All reported security incidents and active investigations will be monitored by the Company Directors. An appropriate investigation and action plan will be prepared and agreed with a representative of the Company Senior Management Team.

Within the provisions of the UK Law, the Company reserves the right at an time to intercept and monitor communications in accordance with the Regulation of Investigatory Power Act; The Telecommunications (Lawful Business Practise) (Interception of Communications) Regulations. The above legislation will be implemented in compliance with the Company monitoring provisions.

Monitoring and recording of electronic communication and data will be carried out in accordance with current Company Policy and interception / monitoring of individual activity shall normally only take place with prior express approval of the Company Directors, but may be undertaken without any prior notice to the users of the Company systems. Permission for undertaking monitoring or surveillance of user activity may in the first instance be given verbally. Any such permission must be recorded in writing as soon as practical. This requirement is to ensure an auditable investigatory process exist for a subsequent disciplinary or criminal proceedings.

4.6.3 Security Incident Management / Investigation

The senior member of staff identified as being responsible for investigating the incident will ensure that all steps are taken to limit damage and loss of data whilst preserving the reputation of Think Learning.

The IT Manager will maintain written procedures for the operation (e.g. start up, backup, show down and change control) of those Company Key Business Systems where threat, risk and organisational impact would adversely the operational effectiveness or organisational reputation.

5 Physical and Environmental Security

Controls will be implemented as appropriate to prevent unauthorised access to, interference with, or damage to information assets.

5.1 Physical Security

Our systems and associated information and media adhere to the government's 'Official' security classification where we have implemented the required controls for ISO27001: 2022 information security management, and Cyber Essentials Plus, security management. We also conduct routine penetration testing on all of our servers.

Computer systems and networks will be protected by suitable physical, technical, procedural and environmental security controls.

File servers and machines that hold or process high criticality, high sensitivity or high availability data are managed by specialist third parties, and contracts with these third parties include a requirement to locate hardware in suitable environments with suitable physical security . All Key Business Systems will be subject to security measures which supports the Company's Continuity Plan.

6 Communications and Operations Management

Controls will be implemented to enable the correct and secure operation of information processing facilities.

6.1 Documented Operating Procedure

Design, build and configuration documentation will be produced in respect of system platforms. Sensitive documentation will be held securely and access restricted to staff on a need to know basis.

6.2 Segregation of Duties

Access to Key Business Systems and key data and information will only be granted based on the user role and access clarification.

When deemed necessary segregation of duties between operations and development environment shall be strictly maintained and all work on Key Business Systems will be strictly segregated.

Permanent and full access to live operating environments will be restricted to staff on role-based requirements.

6.3 System Planning and Acceptance

6.3.1 System Changes

All changes to live Key Business Systems will follow a predefined change management process, to ensure that activities are undertaken in accordance with stringent change control processes and with, where relevant, client sign-off

6.3.2 Controls Against Malicious Software

Controls will be implemented to check for malicious or fraudulent code begin introduced to Key Business Systems.

Source code written by contractors and staff will be subject to security scrutiny before being installed on any line Key Business System.

All systems will be protected by a multi-level approach involving firewall, email scanning, and virus and spy/malware protection on all workstations on the Company network.

All Company workstations will have the appropriate anti-virus software installed and set up to update anti-virus signatures automatically. This must not be turned off by users. Any device found to pose a threat to data or the provision of the Company network will be isolated from the Company network until the security issues are resolved.

Staff and suppliers may use their own PC hardware to connect to the Company systems.

Network traffic will be monitored for any anomalous activity which may indicate a security threat to the network.

6.3.3 Virus Protection

A Virus Protection procedure will be implemented to prevent the introduction and transmission of computer viruses both within and from outside the Company. Failure to maintain a device in a state which prevents or detects virus infection will

leave the device liable to exclusion from the Company network until the security issue is resolved.

6.3.4 Security Patches Fixes and Workarounds

The Information Security Manager will be responsible for ensuring that all suppliers of cloud-based services are implementing security patches and fixes in a timely manner to reduce vulnerabilities to devices within the Company network.

Monthly patching windows will be utilised to ensure the system is up to date on all priority packages.

In addition, ASV scans are performed every three months for all live e-commerce sites, and after every major change.

6.4 IT Housekeeping and Storage

6.4.1 Data Storage

Our systems and associated information and media adhere to the government's 'Official' security classification where we have implemented the required controls for ISO27001: 2013 information security management, and Cyber Essentials Plus, security management. We also conduct routine penetration testing on all of our servers.

System backups will be performed automatically by the relevant systems. The procedure will include keeping backups off site. Periodic checks will be made to ensure backup media can be read and files restored.

Backups protect electronic information from major loss or failure of system software and hardware. Backups are not designed to guard against accidental deletion or overwriting of individual user data files backup and recovery of individual user files is the responsibility of the information owner.

6.5 Network Management

Controls will be implemented to achieve, maintain and control access to computer networks, including wireless LANs.

6.6 Device Decommissioning and Disposal

When a device is decommissioned due to a replacement being purchased, an employee leaving Think or if their employment is terminated by Think, the following steps are taken:

- Data Backup and Transfer:
  - Ensure all necessary data is backed up and transferred securely to secure storage.
  - Erase all data from the laptop's storage devices.
- Decommissioning of Software and Licenses:
  - Uninstall all software applications.
  - Revoke any activated licenses associated with the device.
- Security Assessment:
  - Ensure that all network access credentials and related configurations are removed.
  - Confirm that the laptop no longer has access to any business systems.
- Environmentally Friendly Disposal:
  - If the laptop is not being reused or donated, dispose of it in an environmentally responsible manner.
  - Adhere to the Waste Electrical and Electronic Equipment (WEEE) Directive for electronic waste disposal.
- Compliance Check:
  - Annually review the entire process to ensure it meets the Cyber Essentials Plus requirements.
  - Update the procedure as necessary to comply with evolving standards and laws.
  - Periodically review and update the decommissioning policy to reflect new technological advancements and changes in legal requirements.

6.7 Software Usage and Control

Software will be used, managed and controlled in accordance with legislative and Company policy requirements in relation to asset management and licence agreements.

All major software upgrades and in-house systems development for Key Business Systems will be appropriately controlled and tested through a managed process before live implementation and deployment.

All software used on devices managed by the Company must be installed in compliance with current software licensing policies. Software installed without prior authority and agreement may leave a user liable to prosecution under the Misuse of Computers Act 1990 and disciplinary action.

7 Information Exchange Requests

Use of the Company network will be governed by the Electronic Information Security Policy and the Policy for using IT Resources.

Failure to comply with these requirements will leave a user liable to disciplinary and/or possible criminal legal penalties.

7.1 Exchange of Information with Outside Organisations

Requests by external bodies for the provision of electronic information from Key Business Systems will in all instances be referred to the information owner. This includes Data Subject Access Requests made under the auspices of the Data Protection Action 1998.

Requests for information under the Freedom of Information Act will be referred to the Company Directors. All applications will be handled in accordance with the FOI Application Procedure.

8 Access Control

8.1 Policy Statement

Procedures for the registration and deregistration of users and for managing access to all information systems shall be established to ensure that all users' access rights match their authorisations. These procedures shall be implemented by the IT manager. A periodic review will be conducted to verify user access and roles.

8.2 Think Learning Operational Policy

Access to Key Business Systems will be appropriately controlled and comply with the access rights of the user.

Access to the Company network and IT Services will be restricted according to the access classification of the user.

Company staff, suppliers and external users may use:

- Standard software portfolio;
- Shared file store;
- Email, calendar and public folders;
- Company Business Systems;
- Internet.

8.3 User Responsibilities

Users of the Company network must comply with Company Policies and the Electronic Information Security Policy.

All staff (including agency and temporary staff) must agree to written terms and conditions covering use of IT when they register to use Company IT services.

Personnel Services shall ensure that:

- Confidentiality Agreements form part of the terms and conditions of Employment;
- Awareness training about electronic information security forms part of Company Staff Induction Programmes;
- Information for all staff on electronic information security is maintained in the staff handbook;

The Company must ensure that where there are specific security roles and responsibilities they are documented in all relevant job descriptions and that there is appropriate screening of applicants.

Access to Company systems may be withdrawn and Company disciplinary procedures invoked where a serious or deliberate breach of the policy is made.

8.4 Company Key Business System Access

8.4.1 Subject Access Management and Administration

Formal procedures will be implemented for granting access to both the Company network and IT services. This will be supported by a formal review of user privileges on a regular basis to ensure that they remain appropriate to the role and relationship with the Company. Accounts identified as dormant will be closed.

8.4.2 Password Management

Users are required to use password management software on all devices and follow Cyber Essentials cyber security practice in the selection, use and management of their password and to keep them confidential.

Authorisation of access to Key Business Systems and to the data held by them is the responsibility of the system owner.

System administrator passwords will be issued on the express authority of the IT Manager on a need to know basis. Such password will be changed regularly and when authorised systems administrator **staff leaves.** Network password must be a minimum of twelve characters and the policy on network password complexity will be reviewed periodically.

The account type should at all times reflect the business relationship existing with the member of staff. As a staff member moves to a less formal relationship with the Company then the account associated with that person should reflect this new relationship.

The Company will maintain a list of staff with access to key business systems and services.

8.4.3 Unattended User Equipment

Users of the Company network and IT services are responsible for safeguarding Key Business System Data and sensitive information. In order to protect these information assets, users are required to ensure that devices are not left logged on when unattended and that portable equipment in their custody is not exposed to opportunistic theft, unauthorised access or observation of sensitive information.

Where available, password protected screensavers and automatic log out mechanisms are to be used on systems to prevent individual accounts being used by persons other than the account holders.

9 Compliance

9.1 Compliance with Legal and Company Policy

Supply and use of the Company network and IT services is bound by UK law current at the time of any reported incident. The policy for using IT resources provides guidance on the most common legal and policy requirement pertaining to Company network use.

The IT Manager will maintain and monitor, at six monthly intervals, reports of records of electronic security incidents. Reports will be considered by the Company. It will then be decided if further action or investigation is required.

People who are neither staff nor suppliers do not normally have an automatic right to use the Company network or IT services. Authorisation for such external users will be subject to sponsorship from a member of Company staff along with written agreement from the user to abide by the Company policies. Any outsourcing must include express provisions with respect to IT security and control and any applicable UK law in relation to data processing and confidentiality.

CEO
4th April 2024