POLICY

Information Security policy

Version 6.0
March 2024

This policy is applicable to *all* ICAEW employees including staff in our non-UK offices.

Variation

This document replaces the previous *Information Security Policy* and *is version 6.0*

The following areas have been updated in this version: - PCI Section added for clarity.

CONTENTS

A THE POLICY

INTRODUCTION

Objective

The objective of this Policy is to provide direction and support for information security within ICAEW.

All staff, or those employed by ICAEW are responsible for information security, and for compliance against this policy.

This policy document sets clear direction and demonstrate support for and commitment to information security within ICAEW. It includes such subjects as; main security roles and responsibilities, and mappings to detailed physical, procedural, personnel and technical controls.

An IT Security User Guide accompanies this policy and is aligned accordingly.

Purpose

The purpose of this security policy is to define the protection required of the organisation's assets from all threats, whether internal or external, deliberate or accidental. It also clearly defines the measures taken by ICAEW to protect the confidentiality, availability and integrity of company information and assets.

This policy has been written with the intention of being useful not just to staff responsible for information security but also to the Systems Administrators, Managers and users throughout ICAEW.

All of the information required by ISO/IEC 27002:2022 (the International Standard for Information Security) is contained in this policy document. Not everything will be meaningful to the beginner, however each section will contain something of relevance to the less experienced as well as guidance for managers and technical users. Any questions should direct towards the IT Security Manager.

Scope

This policy describes the measures to be taken to secure ICAEW systems at all ICAEW sites, including Moorgate London, Metropolitan House Milton Keynes, Wolverton Mill Warehouse, Regional Offices, District Societies and International offices and equipment used by remote users. There are some locations residing in rented buildings, e.g. Managed offices, and physical security is maintained by the landlord. The policy details the security measures taken by ICAEW from the external perimeter of the buildings to the electronic environment.

Approval / change conditions

All requests for modification to the security system must first be considered and approved by IT Security Manager & IT Director.

There will also be no variation from this document without the prior approval of the IT Security Manager & IT Director.

The IT Security Manager has direct responsibility for maintaining the policy and providing advice and guidance on its implementation and is supported by IT Security Architect & IT Security Analyst.

Update February 2022

This version of the Information Security Policy is regularly reviewed and updated. There has been a name change to the code of practice which is now ISO/IEC 27002 and the certification standard is entitled ISO/IEC 27001. Current version is - **ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information Security Controls.**

Further information

If you require further information concerning this Policy document, or Information Security in general, please call the ITD Helpdesk on +44 (0)1908 248 080 (Ext 108080).

RISK ASSESSMENT AND TREATMENT

Risk assessment and treatment

Objective: This part of the standard states that regular risk assessments should be conducted to identify, quantify and prioritise risks that are relevant and appropriate to the organisation.

The risks relevant to ITD, which also includes information security risks, are regularly reviewed as part of the existing ICAEW wide process undertaken and managed by ICAEW Governance structure within the Executive leadership team. These risks are reviewed at various levels, including the ITD management team, the departmental teams for their own risks, Data Protection Oversight Group & Executive Leadership Team .

ORGANISATION OF INFORMATION SECURITY

Information security infrastructure

Objective: To manage information security within the organisation

Management information security forum

The Executive Leadership Team is responsible for considering information security risks at regular intervals. Periodic reporting will be provided by Internal Audit or IT Security Manager to update this group on any current security issues and amendments required to the Policy due to legislative or system changes. There are contact points to promote and support Data Protection and Information Security within Departments.

Information security co-ordination

All security matters are co-ordinated and discussed at the appropriate forums.

Allocation of information security responsibilities

There are a number of areas within ICAEW which have responsibility for security these are summarised below and are in line with agreed ICAEW Security model & responsibility matrix:

IT Security Manager is responsible for the following:

- Ensuring the maintenance of and compliance with the Information Security Policy
- Ensuring that the importance of security is communicated to all staff
- Ensuring that physical access to computer equipment is strictly controlled
- Ensuring that periodic written reports are provided on security matters when required
- Maintaining liaison with Internal Audit
- Ensuring that users (internal and external) are aware of the value and sensitivity of the information and take appropriate steps to guard against unauthorised access

Security Architect is responsible for the following:

- Reviewing new and changed applications and services for compliance with security policies and requirements, accessing all cyber security needs for ICAEW.
- Establishing mechanisms to protect against virus infection, unauthorised data destruction and hacking
- Access to systems, information or production software is not available to unauthorised persons through security monitoring.

The ITD Infrastructure Manager is responsible for:

- Ensuring that logical access rights are consistently applied across authorised persons

ICAEW Management Team is responsible for considering information security risks at regular intervals.

The Human Resources Department for any corrective or disciplinary action required due to misuse of ICAEW systems.

The Property Services and Facilities Department for general building security.

The Internal Audit department and external IT auditors include security arrangements in their periodic reviews.

ICAEW Governance within the Executive Leadership Team considers organisational risks on a regular basis.

Managers throughout ICAEW to ensure their staff adhere to security controls and that they receive timely and appropriate training.

Every member of staff, including contractors and consultants, are responsible for safeguarding the information that is vital to the working of ICAEW.

The security framework can be summarised below:-

AREA	RESPONSIBLE
Risk assessment	ICAEW Governance
Security documentation	IT Security Manager
Security forum	Data Protection Oversight Group
Hardware asset management including disposals & auditing	Helpdesk Manager
Software asset management	Infrastructure Manager
Human resources:- – Staff awareness – Staff disciplinary process – Third party awareness/compliance	Helpdesk Manager Director HR IT Security Manager, Security Architect
Physical & environmental security including computer rooms, cabling/network and PC/laptop	IT Security Manager, Security Architect
Anti-virus controls	Infrastructure Manager
Document control process	Head of Web and Systems Development
Network penetration testing	IT Security Manager, Security Architect
Application security reviews	Application Development Manager
Access control	Infrastructure Manager
Access control auditing	Head of Web and Systems Development
Security in new IT systems	IT Security Manager, Security Architect & Business Systems Manager
Security breach call logging	IT Security Manager, Security Architect &

	IT Service Delivery Manager
Major incident process	Helpdesk Manager
Business continuity management	Director IT & Property Services
Data Protection Act compliance	CFO
PCI-DSS Compliance	Accounts Receivable Manager

External third parties will be commissioned at various times to support these activities.

Authorisation process for information processing facilities

All new IT equipment and facilities shall be authorised in line with Asset Management Procedures. To ensure that the asset register remains current, and assets are afforded adequate protection, all new equipment must be purchased or disposed of with authorisation from the Director IT & Property Services.

Specialist information security advice

IT Security Manager & Security Architect are responsible for all cyber security and will provide advice and guidance on the implementation of information security controls and required signoff. Third parties will be used at various times to provide independent specialist security advice and/or testing.

Co-operation between organisations

Security co-operation exists internally with regard to buildings and hardware (ITD and PS&F Departments). E-Mail scanning and Internet Firewalls are managed by a third party. Network Penetration testing of internal and external communications, both voice and data, and the Web site is organised on a regular basis.

Independent review of information security

The Internal Audit department and external IT auditors include security arrangements in their periodic reviews.

Security of third party access

Objective: To maintain the security of organisational information processing facilities and information assets accessed by third parties

Identification of risks from third party access

The Confidentiality, Integrity and Availability of ICAEW's assets shall be protected from legitimate third party organisation connections to ICAEW computer/communications equipment by confirmation that the third party conforms to this security policy and connection has been approved by the Cyber security Team.

Security Requirements in Third Party Contracts (including Outsourcing)
Commercial contracts should be reviewed prior to any contracts being signed and clearly stipulates third party security requirements and approved through contract approval process. All third parties

should complete the required Security questionnaire document which is available via IT Security Manager for assessment and approval.

Where possible, all third parties shall be ISO/IEC 27001 certified by an Accredited Certification Body or working towards the standard or equivalent security accreditation and where required they should be registered under the current Data Protection Act Legislation and any other applicable legislation. A comprehensive list of considerations is contained in Appendix A.

ASSET MANAGEMENT

Accountability for assets

Objective: To maintain appropriate protection of organisational assets.

Inventory of assets

The location of all assets shall be listed and held by ITD. This inventory is used for financial as well as security reasons and is held in ServiceNow.

Information classification

Objective: To ensure that information assets receive an appropriate level of protection

Classification guidelines

Assets shall be classified according to their Confidentiality, Integrity and Availability values and in accordance with Data Classification policy and determined by the damage that could accrue to the organisation if the assets were to be disclosed, changed or lost. Appropriate levels of security are afforded to assets dependent on their sensitivity.

Information labelling and handling

Sensitive information and outputs from systems handling sensitive data shall be labelled appropriate to their sensitivity or criticality to ICAEW. This is the responsibility of the originator of this material.

HUMAN RESOURCES SECURITY

Security in job definition and resourcing

Objective: To reduce risks of human error, theft, fraud or misuse of facilities.

Including security in job responsibilities

ICAEW personnel should be aware of the security implications of all legislation with a bearing on them, including the Data Protection Act 2018, and the Computer Misuse Act 1990, which affects both ICAEW and the individual. Their attention to these responsibilities shall form part of the Terms of Contract.

In addition, ICAEW employees shall be measured against objectives set as part of their role profile, which where appropriate will include security aspects, including adherence to the information security policy.

Personnel screening and policy

Screening/background checks shall be carried out on all employees in accordance with current HR procedures.

Checking of temporary staff on short term assignments shall be the responsibility of the agency from which they are hired, although ICAEW reserve the right to carry out further checks at their discretion. Other agency staff shall be liable to the same screening process as permanent staff.

Confidentiality agreements

Third parties will complete a Confidentiality Statement which must be observed before access is permitted to ICAEW data/information. A copy of the Confidentiality Statement can be found in Appendix D.

Terms and conditions of employment

General Terms and Conditions of Employment are outlined in HR policies held on the intranet. Terms and conditions of employment include the employee's legal responsibilities regarding:

- Data Protection Act 2018
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000 (users' communications may be subject to monitoring and recorded)
- Copyright, Designs and Patents Act 1988
- Financial Services Act
- Telecommunications Acts 1984 & 1997
- Electronic Communications Act 2000
- Competition Act 1998

A précis of key legislation can be found in Appendix B.

In addition, employee Terms & Conditions include:

- A clause, which clearly states that all work produced during the course of the employment, becomes the property of the organisation, including any intellectual property rights and copyright attributes

- Confirmation that an employee's responsibilities are extended outside the office and outside working hours (e.g. in the case of home working)
- Conflict of Interest Disclosure
- Statement of Terms of Employment.

Leavers

All ICAEW property shall be returned when an individual leaves ICAEW. ICAEW property shall in this instance be defined as all hardware, software, documentation, passes, phones and any other material items provided by or through ICAEW. There is a process where HR informs various departments of an individual's leaving date, which prompts the actions to be taken to recover all ICAEW property.

User training

Objective: To ensure that users are aware of information security threats and concerns, and are equipped to support organisational security policy in the course of their normal work.

Information security education and training

Every member of staff shall receive documentation outlining, in addition to health & safety, a summary of security awareness responsibilities which shall include:

- The purpose and content of the IT security policy
- Password management
- Unattended terminals
- Printouts
- Viruses
- Copying
- Backups
- Physical security
- Third party systems
- Incident reporting

Monitoring Electronic Communications

ICAEW reserves the right to intercept and/or monitor and/or record, and wherever necessary, review the history of communications made by you via any of its electronic communications systems, this includes email, telephone (in particular, calls to and from ICAEW helplines) and internet use. This also includes 365 services such as MSTeams.

This is to ensure that our systems are used primarily to further the business of ICAEW, that they are not used for inappropriate and/or unlawful purpose and that system capacity is sufficient for the needs of the organisation.

The content of communications will be monitored only where necessary. However you should be aware whilst we respect privacy such monitoring may take place and that the content of your communications using ICAEW systems cannot therefore be regarded as completely confidential.

For more information, please consult the Electronic Communications Monitoring Policy which is available on the Intranet.

Responding to security incidents and malfunctions

Objective: To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

Reporting security incidents and weaknesses

All personnel shall be aware that they must report any security incident or weakness to the ITD Helpdesk, in accordance with IT Security User Guide. No attempt is to be made to circumvent procedures. Logged security incidents will be monitored by ITD on a regular basis. Unauthorised personnel shall make no attempt to explore and attempt to repair any security incident/weakness.

Reporting software malfunctions

Personnel shall be aware that they should report operational software malfunctions to the ITD Helpdesk.

Disciplinary process

This Security Policy provides an extension to the terms and conditions of employment. Violations of this Policy will be handled in a manner consistent with comparable situations requiring corrective or disciplinary action.

PHYSICAL AND ENVIRONMENTAL SECURITY

Secure areas

Objectives: To prevent unauthorised access, damage and interference to business premises and information.

Physical security perimeter

There are a number of buildings occupied by ICAEW staff and these are summarised below:

- Metropolitan House, Milton Keynes
- Chartered Accountants Hall, Moorgate Place London
- Wolverton Mill Warehouse, Milton Keynes
- International Offices (Brussels, Dubai, Singapore, Beijing, Hong Kong and Kuala Lumpur)
- Regional offices (Bury St. Edmunds and Sheffield)
- District Societies

There are some locations residing in rented buildings, e.g. managed offices, and physical security is maintained by the landlord.

In addition, there are a number of home workers who either work full or part of the time from home. Guidelines are available from the Property Services and Facilities department.

Physical entry controls

- **Company site**. A single entrance to the main buildings is controlled by reception. A sponsor shall notify reception of all intended visits. Visitors should only enter the building through the main entrance.
- **Offices**. In the majority of cases entry to the main offices is controlled by an electronic swipe card (badge reader) or key code lock, which is enhanced by an exterior CCTV camera system and DVST (Digital Visual Storage Transmission). All premises access must be granted on a "need only" basis. Contract staff will be issued with cards for the period of their contract. Swipe card access shall only be granted or extended on instructions from the relevant head of department or deputy. Periodic checks will be made to determine swipe cards not used in the period so that they can be deleted from the system. There are some locations residing in rented buildings, e.g. managed offices, and physical security is maintained by the landlord. Security passes must be worn at all times.
- **Fire exits / escapes**. Although fire exits are not a normal means of ingress/egress personnel are not to use any fire exit unless in an emergency or as directed by a senior member of staff or appointed fire warden.
- **Visitors**. Visitors shall be met by their sponsor and be booked in at reception. They are to be escorted at all times unless permission for unescorted access has been specifically granted by the sponsor. All visitors shall be identifiable by wearing the security badge issued at reception. When they leave, visitors should be escorted to the building exit and security badges handed in to reception
- **Windows**. When the offices are vacated at the end of the day, checks shall be carried out, as part of general office security procedures, to ensure that all windows and other means of ingress are closed and secured prior to setting the alarm systems.

Securing offices, rooms and facilities

Access to secure areas, e.g. data centres, is strictly limited to authorised personnel. They will be locked at all times. Nominated personnel only shall be in possession of any digital lock combinations or swipe card permissions.

In addition, where appropriate, secure areas should be afforded additional environmental controls. Examples of this are below:

- Regular checks to ensure areas are clear, tidy and free from dust and combustibles.
- Monitoring of the environment to be able to respond to any overheating problems that may occur.
- In the case of computer media, ensuring that disks are acclimatised before loading to prevent condensation problems.

Working in secure areas

Unsupervised working within secure areas should be kept to a minimum. Third party support services personnel will be escorted and monitored when working in these areas.

Isolated delivery and loading areas

Delivery and loading areas will be isolated and secured so that no unauthorised access is possible. This is especially important where these areas are near to information processing facilities.

Equipment security

Objectives: To prevent loss, damage or compromise of assets and interruption to business activities.

Equipment siting and protection

Care is taken to ensure that the physical siting of equipment avoids damage or inadvertent loss. ICAEW offices are protected by security alarms, which are monitored when set, and a response is provided should the alarm activate. Security documentation sets out guidelines for laptop/remote users on equipment care and security, and remote working arrangements.

Critical equipment such as servers, network switches shall be afforded much higher security considerations in that they shall be secured in a separate environment under strict access control measures.

Power supplies

Power supplies are under the control of the Property Services and Facilities department. Important computer equipment, where identified, shall be protected from power surges/burnout/failures etc., by Uninterruptable Power Supplies (UPS).

Cabling security

Telecommunications lines are under the control of ITD Infrastructure personnel. Cabling shall be protected from unauthorised interception or damage by using appropriate conduit.

Communications cables are to be protected from interference caused by power cables with appropriate separation.

Equipment maintenance

No equipment requiring repair shall be removed from site without prior approval. Agreements with third party contractors (including vendors) shall cover the possibility, and therefore the confidentiality, of sensitive information remaining on equipment such as computers, personal digital assistants, photocopiers etc.

Security of equipment off-premises

When appropriate authority has been given to ICAEW staff to use computer equipment off site, they shall be held responsible for its safety and security.

Secure disposal or re-use of equipment

Floppy disks, tapes and computer equipment shall be disposed of securely. Equipment for disposal, and equipment that is being re-used, shall have all information securely erased. There is a specialist company who arrange for the collection and disposal of redundant equipment in accordance with the WEEE Directive. The selling off/giving of equipment to ICAEW staff will be discouraged as it seems that there is not a consistent approach to the removal of data and there is an implied guarantee on the equipment's functionality and/or safety, which ICAEW cannot possibly fulfil.

General controls

Objectives: To prevent compromise or theft of information and information processing facilities.

Clear desk and clear screen policy

ICAEW adopts a clear desk policy which is felt best practise. All sensitive papers and computer media shall be stored in filing cabinets or store cupboards, preferably locked, when not in use. A screensaver will be implemented on computers at the configuration stage, which will activate after 10 minutes. This is locked down and cannot be changed.

Removal of property

No property, equipment, data or software is to be removed from ICAEW without prior authorisation. Return of all equipment must also be adequately logged.

COMMUNICATIONS AND OPERATIONS MANAGEMENT

Operational procedures and responsibilities

Objectives: To ensure the correct and secure operation of information processing facilities.

Documented operating procedures

Procedures and records shall be established and maintained to cover all aspects of the operation and management of ICAEW systems and network.

Operational change control

Changes to information processing facilities and systems shall be controlled. All live changes shall be formally processed through the Change Control Procedures, including approval by the ITD Change Advisory Group.

Incident management procedures

Procedures and records shall be established for the reporting of major system incidents, such as a significant loss of service and security breach reporting.

Segregation of duties

Key personnel shall not be placed in such a position of responsibility that by their absence ICAEW cannot operate efficiently, unless it is considered impractical to do so.

Separation of development and operational facilities

Development and testing activities may cause unintentional changes to software and data sharing the same environment. Segregation of development, test and operational environments shall be implemented in order to minimise the risk of negligent or deliberate system misuse and the propagation of errors between environments.

External facilities management

The use of external contractors exposes ICAEW to additional security risks and these should be identified at an early stage. Therefore, all facilities management contracts shall include:

- A mandate to implement and audit the requirements of this security policy document
- Controls to protect the business from the additional exposure resulting from the external management of ICAEW systems
- As a minimum, the requirement for compliance with or working to the principles of ISO/IEC 27002

System planning and acceptance.

Objectives: To minimise the risk of systems failure.

Capacity planning

The ITD Infrastructure Team shall regularly monitor capacity requirements to avoid failures because of inadequate capacity on IT systems. Future requirements, based on monitoring and experience shall take into account new business, system requirements and projected trends within ICAEW’s information processing systems. Due consideration shall be given to security aspects when planning ahead.

System acceptance

Where applicable hardware and software shall have been methodically tested as follows:

- Performance and capacity requirements
- Preparation of disaster, fall-back and recovery plans
- Preparation and testing of operational procedures
- No-adverse impact on other systems
- User training (where applicable)
- Does not introduce added security risks
- Functions according to design specifications
- Does not adversely affect the operation of the system
- Introduces no unauthorised system change
- No trapdoors, other malicious code, or known security weaknesses exist, or those that exist have been patched

Protection from malicious software

Objectives: To protect the integrity of software and information

Controls against malicious software

All ICAEW systems have loaded an anti-virus scanner that provides an aggressive check for viruses and other malicious code on a frequent basis. However, to avoid malicious code being loaded onto ICAEW systems no software, irrespective of origin, particularly media from computer magazines, is to be loaded onto any ICAEW system without the express approval of the ITD Infrastructure Team. In addition:

- The ITD Infrastructure Team shall not load any software until they have confirmed its licensing arrangements
- The ITD Infrastructure Team shall not load any software unless it has undergone vigorous anti-virus scanning beforehand
- Anti-virus scanning programs shall be updated as frequently as advised by the vendor, by the ITD Infrastructure Team
- Any suspicion of a virus attack is to be reported in accordance with incident reporting procedures

It is the responsibility of remote users to ensure that they follow the correct anti-virus procedures as defined by the ITD Infrastructure Team.

All staff should ensure continued vigilance surrounding viruses especially when receiving unsolicited messages with executable attachments. In addition, staff should make sure that anti-virus software is installed on their machine and check all disks for viruses before use.

Housekeeping

Objectives: To maintain the integrity and availability of information processing and communication services.

Information backup

Backup copies of applications and data ensure continuation of processes should a malfunction occur. Backups shall bear an identifying mark to determine its origin, and the type of backup. Backup labels shall not specify the type or identity of the data being held on the media.

- **Application programs**. Most application software licensing allows a working copy of the program to be made. The ITD Infrastructure Team shall make working copies of all software and store the originals in the secure off-site location.
- **Data files**. The ITD Infrastructure Team shall be responsible for taking daily backups of data files on a rotational basis
- **System files**. A full system backup shall be taken
- Testing. Tests of all backup types shall be carried out by the ITD Infrastructure Team at frequent intervals
- **Audit**. The ITD Infrastructure Team shall conduct regular audits of backup media
- **User responsibilities**. All staff should make sure that backups are taken of their data files either by storing them on the network drives or making copies if they have to store them on their local C drive (this is particularly important for Notebook users)

Operator logs

Logs shall be maintained by the ITD Cyber Security Team of work carried out and retained for a minimum of 6 months. Regular independent checks of the logs shall be conducted and the logs will include:

- System starting and finishing times
- System errors and corrective action taken
- Confirmation of the correct handling of data files and computer output.
- User behaviour monitoring that includes system access times and locations

Fault logging

Users reporting problems with information processing or communications systems shall report faults to the ITD Helpdesk. The ITD Infrastructure Team shall record faults and actions taken in the Operator Log.

Network management

Objectives: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

Network controls

ICAEW systems shall be administered (by the ITD Infrastructure Team) such that access and resource controls are allocated on the basis of minimum privilege. Security monitoring shall be regularly carried out to identify security incidents.

Media handling and security

Objectives: To prevent damage to assets and interruptions to business activities.

Management of removable computer media

To prevent damage to assets and interruptions to business activities, access to media shall be controlled and that media physically protected.

Disposal of media

It is a common misconception that formatting media ensures removal of data files. This is factually incorrect, since commercially available tools are available to resurrect "destroyed" sensitive data. Therefore, all media for disposal shall be destroyed securely.

Information handling procedures

Procedures will be established for the handling and storage of information to protect against unauthorised disclosure or misuse.

Security of system documentation

Access to system documentation provides tools for any potential attacker. Therefore, the ITD Infrastructure Team shall secure all system documentation when not in use.

Exchanges of information and software

Information and software exchange agreements

Any information exchanged internally or to other organisations is controlled by the registration under the Data Protection Act. ICAEW is following government guidelines on 'life cycle' information exchange. This topic will therefore require periodic review to keep up with government legislation and guidelines.

Security of media in transit

There will be controls in place to protect media in transit from unauthorised access, misuse or corruption. This will cover document collection and delivery, ordering and delivery of IT equipment, media handling and security and installation of hardware and software.

Electronic commerce security

Electronic commerce currently extends to member's subscriptions and faculty membership, which are processed via a secure third party site. The Finance and Members Registration departments have administration rights to set prices.

Security of electronic mail

Security controls will be applied to the use of electronic mail in accordance with ICAEW Email policy. ICAEW reserves the right to retrieve the contents of messages sent over its Email and Web facilities to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts or to comply with any legal obligation.

Publicly available systems

There will be procedures and processes to protect the information published on ICAEW Internet and Intranet such that confidentiality, integrity and availability are maintained.

Other forms of information exchange

See section ‘Information and Software Exchange Agreements’.

External data interfaces

The ITD ‘Interface Policy’ defines the method and controls regarding the implementation of data interfaces with external suppliers with ICAEW.

ACCESS CONTROL

Business requirement for access control

Objective: To control access to information.

Access control policy

Access to network services and data shall be controlled on the basis of documented business requirements. The following rules shall apply:

- Access to system resources shall be on a strict need-to-know basis
- The ITD Infrastructure Team shall receive the necessary training
- User profiles shall be standardised
- Critical information related to the business applications shall be identified
- All staff shall follow and abide by relevant legislation and any contractual obligations regarding protection of access to data or services
- To avoid a potential security weakness, all installation time accounts shall be disabled and default passwords changed.
- In distributed and networked environments, trust should not be propagated in an uncontrolled way. Connections to external networks, including the Internet, should be of a consistent level of security
- Monitoring (auditing) of the Security Policy and permission settings shall be enforced continuously by the ITD Cyber Security Team and will be assisted by records maintained on the Helpdesk system
- Originators of data files shall be owners by default and shall be responsible for saving the file in the appropriate directory to ensure only appropriate personnel have access.

User access management

Objective: To prevent unauthorised access to information systems.

User registration

The user’s Head of Department or deputy shall authorise in writing and make the ITD Helpdesk aware of the requirement to change access rights. When a user (permanent, temporary or contractor) no longer requires access to the network or system resource the ITD Helpdesk shall be informed immediately and the user profile will be removed in accordance with the ITD Leavers procedure. Each new user will be briefed on User ID and password use.

Privilege management

The ITD Infrastructure Team shall enforce access and privileges to files and resources on a strictly need-to-know basis.

User password management

Passwords shall be issued in line with documented ITD procedure.

Review of user access rights

The ITD Infrastructure Team and the ITD Cyber Security Team shall maintain effective control over access to data and information services and conduct a formal process regularly to review users' access rights.

User responsibilities

Objective: To prevent unauthorised user access.

Password use

Users shall be aware that they are responsible for ensuring the safety and integrity of their individual passwords as defined in the IT Security User Guide. As such, passwords shall be of a length and composition mandated by the ITD Cyber Security Team i.e. minimum 8 alpha numeric characters with a combination of upper and lower case characters, automatic enforced change after 45 days.

Unattended user equipment

Time-lapse screensavers shall activate on all systems within 10 minutes of inactivity to negate unauthorised access. Unless specifically identified as a special or critical system component all systems are to be switched off when the session has ended.

Network access control

Objective: Protection of Networked Services.

Policy on use of network services

It is necessary to ensure that connected users of computer services do not compromise the security of any networked service. Users are able to connect to the Internet via their desktops and therefore services must be strictly controlled. This is achieved by use of a firewall. The firewall shall be configured in accordance with advice from ITD's security advisors. At present, the firewall is managed by Orange Cyber Defence

Enforced path

The network must only route users to pre-defined authorised destinations i.e. applications or services.

User authentication for external connections

Remote users must be identified and authenticated by the operating system before connecting to internal systems and networks.

Node authentication

Before access is allowed to internal systems and networks, remote computer systems must:

- Be identified and authenticated by the system
- Authenticate their users with a confidence/assurance that is at least equal to the strongest mechanism used by the system being accessed

Remote diagnostic port protection

Any remote diagnostic port shall be password protected.

Segregation in networks

ICAEW system is not large enough to be segregated. Although the network will be a single domain model, if required, users shall be segregated from applications, resources and data files by group and individual permissions.

Network connection control

The approved systems that may connect are agreed by the ITD Management Team and no connection between ICAEW system and any other system will be permitted without formal approval from the ITD Management Team.

Bring your own device

The Bring Your Own Device (BYOD) policy defines the standards, procedures, and restrictions for staff that connect a personally-owned device to ICAEW's corporate network for business purposes. The policy applies, but is not limited to all devices and accompanying media that fit the following classifications:

- Smartphones
- Other mobile/cellular phones
- Tablet computers
- Portable media devices
- Laptop/notebook computers, including home desktops
- Any personally-owned device capable of storing corporate data and connecting to a network

Network routing control

ITSEC (IT Security Evaluation and Certification Scheme) evaluated firewalls control access.

Security of network services

Adequate redundancy shall be built into the network to ensure that availability satisfies agreed service levels.

Operating system access control

Objective: To prevent unauthorised computer access.

Automatic terminal identification

Not applicable.

Terminal logon procedures

No system shall permit access unless the user has supplied a valid User ID and password (if working externally from the ICAEW Offices a valid MFA code must also be supplied), and:

- The system shall not grant access unless both parts (User ID and password) are both correct
- The system shall not display the password in clear text
- The system shall not display the last User ID
- The system shall not identify to the user which if any part of the logon process is valid or partially valid
- The system shall permit only 8 logon attempts before lockout which can only be restored after line manager authorisation via email to the ITD Helpdesk
- The User ID and password should not be stored or divulged together.

User identification and authentication

Each user shall be given a User ID that conforms to ITD's naming convention.

Password management system

All users shall comply with the password management rules (IT Security User Guide refers). Passwords should not use the names of friends, family, pets, objects in the user's environment, or anything else that may be readily guessed or otherwise ascertained.

Use of system utilities

The ITD Cyber Security Team shall strictly enforce access to system utilities.

Duress alarm to safeguard users

Not applicable.

Terminal timeout / limitation of connection time

Not applicable.

Application access control.

Objective: To prevent unauthorised access to information held in information systems.

Information access restriction

Access to data files and resources is controlled in that users will be given access rights and permissions on a need-to-know basis. Users automatically become the owners of data files they originate and access rights are automatically set appropriately.

Sensitive system isolation

Not applicable.

Monitoring system access and use

Objective: To detect unauthorised activities.

Event logging

The network provides tools for the monitoring of events, some by default and others with ITD Cyber Security intervention. Logs are to be retained for a minimum of 90 days. The ITD Cyber Security Team shall ensure that the following default logs are enabled:

- Any attempt to disable or change the settings of the system monitoring tool

- Start-up parameters and any changes to them
- System or Application start-up and shut-down
- Failed login attempts
- Rejected attempts because of insufficient authority
- Unauthorised access or use of a system resource

Monitoring system use

System and application use and attempted use shall be monitored by the ITD Security Team to ensure the integrity of ICAEW systems. All staff will be made aware of Security Breach/Weakness reporting via the IT Security User Guide.

All events in the audit data shall be taken into account when deciding what to audit and the appropriate actions to take. The following shall be monitored:

- Enabling and disabling of the audit process
- Any changes to the type of events logged by the audit trail
- Start-up parameters and any changes to them
- System and application start-up and shut-down
- Successful login attempts e.g., logon patterns
- Rejected access attempts because of insufficient authority e.g., wrong User ID/password
- Use of selected transactions

Clock synchronisation

ICAEW IT systems shall be synchronised.

Mobile computing and teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities.

Mobile computing

Security and best practise control responsibilities are explained to users when mobile facilities are delivered to them (e.g. laptop, mobile, smartphone, Wi-Fi usage).

Teleworking

A procedure for remote working is passed to the user along with the delivery of the laptop. This details connection and disconnection steps when accessing central systems.

INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

Security requirements of systems

Objective: To ensure that security is built into information systems.

Security requirements analysis and specification

This security policy document should be reviewed regularly or where system configuration requires new input or the current policy directions are no longer valid.

Any proposed changes to the Intranet/Internet shall be fully discussed at the ITD Management Team to ensure that its level of protection (Assurance Level) remains the same.

Significant changes to IT facilities (H/W and S/W) shall be reviewed to ensure that they pose no additional risk to ICAEW. This review shall include:

- A business input against ICAEW IT planning
- A technical input, including review against ICAEW IT strategy
- A financial input against ICAEW budgets

Security in application systems

Objective: To prevent loss, modification or misuse of user data in application systems.

Input data validation

The integrity requirements of data should be enforced through data input validation built into any business systems.

Control of internal processing

All applications shall be designed to minimise the risk of corruption by processing errors by building in validation checks, reconciliation checks etc. where necessary.

Message authentication

Not relevant at this time.

Output data validation

The validation of data in application systems e.g. reconciliation, will be part of the project management process for acceptance of new systems.

Cryptographic controls

Objective: To protect the confidentiality, authenticity or integrity of information.

Policy on the use of cryptographic controls

Cryptographic controls are used for the transfer of financial data between ICAEW and external organisations and include member's subscriptions and faculty membership via the Web site. Encryption is also being used for FTP (File Transfer Processing) and connections to Regional

Offices. Further use of encryption will be considered as and when any risks associated with data movement require it.

Encryption

See section ‘Policy on the Use of Cryptographic Controls’.

Non repudiation services

Not relevant at this time.

Key management

Not relevant at this time.

Security of system files

Objective: To ensure that IT projects and support activities are conducted in a secure manner.

Control of operational software

All software shall be tested before being introduced into an operational environment. Before use, all original software shall be copied to provide working copies. Original copies are to be stored securely and should never be used unless required to renew corrupt working copies.

Formal procedures shall be followed to upgrade systems software or load patches. The loading of software onto any ICAEW equipment without the approval of the ITD Infrastructure Team and the ITD Cyber Security Team is expressly forbidden e.g. upgrading the desktop browser before ITD have formally had sign off that the browser works with all ICAEW web based systems.

Protection of system test data

System test data shall be protected and controlled. Items that must be considered are:

- access controls, which apply to operational systems, must also apply to test systems
- there must be an authorisation process and log maintained each time operational information is copied to a test system
- operational information will be erased from a test system and refreshed on a regular basis
- where practical, information on test systems should be ‘depersonalised’ before use

These controls may have to be reviewed in the future in light of any legislative requirements.

Access control to program source library

The ITD Infrastructure Team shall control access to application programs, development software and source code.

Security in development and support processes

Objective: To maintain the security of application system software and information.

Change control procedures

All changes to live software and hardware shall be appraised from a security perspective by the Change Control Advisory Group.

Technical review of operating system changes

When changes occur, the operating systems shall be reviewed to ensure that there is no adverse effect on security.

Restrictions on changes to software packages

Vendor supplied software packages shall not be modified outside of the scope recommended by the supplier.

Covert channels and trojan code

Trojan code is designed to affect a system in a way that is not noticed and not required by the recipient or user of the program. Correct configuration of the firewall and use of content scanning can contain this type of threat. However, any unauthorised change to the firewall will bring inherent dangers.

Additional security monitoring through tools such as LogRhythm CloudAI & Varonis analytics provide real-time alerting to the IT Security team.

The ITD Security Team shall ensure that the firewall management company notifies them when a suspected attack occurs. Checks of the firewall logs are to be carried out as part of routine checks.

Outsourced software development

Appendix A details what security measures should be requested in any outsourcing contract and this will be reflected in the tendering process.

INFORMATION SECURITY INCIDENT MANAGEMENT

Information security incident management

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action.

There are defined security responsibilities within the organisation from the Director IT & Property Services and Management Team on the policy and risk assessment aspects through to the Infrastructure, Web/Application Development & Support teams on technical responsibilities. There are specific responsibilities within the Helpdesk for gathering and reporting security incidents and the Business Analysis team for taking account of information security at the early stages of a project. The information security controls are also independently reviewed at regular intervals via Internal Audit, ICAEW IT external auditors and other third parties when performing specific reviews.

Security breaches are a call category on the Helpdesk system and these are reviewed and reported on a regular basis. The reporting of security breaches is mentioned within the IT Security User Guide.

There is a major incident procedure which has been invoked on a number of occasions where there has been a significant loss of an operational service. These major incidents have included security breaches.

BUSINESS CONTINUITY MANAGEMENT

Aspects of business continuity management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

Business continuity reduces the damage caused by disasters and security failures (which may be caused by, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventative measures. Various aspects will be tackled as part of this process:

- documenting the criticality and loss impact of IT systems, reviewing this on a regular basis and taking into account business continuity as part of new system acceptance and implementation
- defining business continuity/disaster recovery strategies and ensuring arrangements are in place, either internally or with third party suppliers and making sure this is reviewed on a regular basis so as to match the business requirements
- documenting business continuity plans and making sure these are reviewed on a regular basis
- periodic testing of the business continuity plans taking into account new or changed systems
- user departments should agree contingency plans in their area to be used in case of disruption or disaster

COMPLIANCE

Compliance with legal requirements

Objective: To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements.

An overview of key legislation can be found in Appendix B.

Identification of applicable legislation

The design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements. All relevant statutory, regulatory and contractual requirements shall be explicitly defined in ICAEW policy documentation. The specific controls and individual responsibilities to meet these requirements shall be similarly defined and documented in the security policy. Two of the main legislative requirements are the Data Protection Act (2018) and the Computer Misuse Act (UK) 1990. The former is described later and the main requirements of the Computer Misuse Act (UK) 1990 are described here:

Computer misuse

The main provisions of the Computer Misuse Act (UK) 1990 are that:

- **Section 1**. A person is guilty of an offence if he/she causes a computer to perform any function with intent to secure access to any program or data held in any computer and that the access he/she intends to secure is unauthorised. The intent a person has to have to commit an offence under this section need not be directed at any particular program or data held in any particular computer.
- **Section 2**. A person is guilty of an offence under this section if he/she commits an offence under section 1 above ("the unauthorised access offence") with intent to commit an offence to which this section applies or to facilitate the commission of such an offence (whether by himself or by any other person) and the offence he/she intends to commit or facilitate referred to in this section as the further offence.
- **Section 3**. A Person is guilty of an offence if he/she commits any act which causes an unauthorised modification of the contents of any computer and at the time when he/she does the act he/she has the requisite intent and the requisite knowledge. The requisite intent is intent to cause a modification of the contents of any computer and by so doing to impair the operation of any computer, to prevent or hinder access to any program or data held in any computer, or to impair the operation of any such program or the reliability of any such data. The intent need not be directed at any particular computer, any particular program or data or a program or data of any particular kind, or any particular modification or a modification of any particular kind.

Intellectual Property Rights (Control of Proprietary Software Copying)
The ITD Infrastructure Team shall, where possible, make working copies of software, storing the originals securely off site. No other copies may be made and the use of illegal software is forbidden. Offenders shall be the subject of disciplinary action.

Safeguarding of organisational records

Key records shall be identified and secured appropriately. Storage facilities that should be considered include:

- fireproof safes/cabinets

- locked cabinets/draws
- microfilm
- list maintenance e.g. software licences, contracts

Data protection and privacy of personal information

The UK has introduced legislation placing controls on the processing and transmission of personal data (generally information on living individuals who can be identified from that information). Such controls impose duties on those collecting, processing and disseminating personal information, and may restrict the ability to transfer that data to other countries. The Data Protection Act 2018 has strict compliance requirements for electronic and paper records. The main responsibilities are as follows:

Data Protection Officer's responsibilities

Compliance with data protection legislation requires appropriate management structure and control. In accordance with that role's Terms of Reference the DPO shall provide strategic guidance to managers, users and service providers on their individual responsibilities and the specific procedures that should be followed.

Data owner's responsibilities

Owners of data shall inform the data protection Team about any proposals to keep personal information in a structured file, and to ensure awareness of the data protection principles defined in the relevant legislation.

Prevention of misuse of information processing facilities

The information processing facilities at ICAEW are provided for business purposes. Restrictions on use are outlined in individual reference documents. However, personnel using any of these facilities for non-business or unauthorised purposes, without management approval and supporting accounting arrangements may face disciplinary action. The retrieval or propagation of obscene material may be a criminal offence. ICAEW will offer full co-operation to the authorities in such cases.

Regulation of cryptographic controls

See section 'Policy on the Use of Cryptographic Controls'.

Collection of evidence

It is necessary to have adequate evidence to support an action against a person or organisation and therefore the necessary guidelines for the collection and safeguarding of such evidence will be in place. Internal Disciplinary Procedures will be used for any disciplinary action that may arise from the collection of any evidence.

Payment Card Industry Data Security Standard Compliance

Payment Card Industry Data Security Standards (PCI-DSS) is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data.

It consists of a number of steps and security best practices that help to ensure the secure processing of sensitive data throughout ICAEW, and ICAEW has an obligation to protect confidential cardholder information through compliance with PCI DSS.

Failure to comply with these regulations could result in cardholder data becoming compromised, data security breaches, substantial fines, severe reputational damage and/or the loss of income, and potentially the revoking of ICAEW's authority to accept card payments.

Definitions

PCI DSS is concerned with account data for debit and credit cards. Account data is made up of cardholder data and sensitive authentication data (also known as sensitive information), and there are specific rules around the use, storage and transmission of these two types of data.

Cardholder data refers to the card number across the centre of the card (otherwise known as the Primary Account Number, or PAN), the cardholder name, the expiry date and the service code (also known as the security code or card validation value - CVV).

The PAN is the defining factor for cardholder data. If the cardholder name, service code, and/or expiry date are stored, processed or transmitted with the PAN, they must be protected in accordance with the PCI DSS requirements. Storage of cardholder data is permitted but must always be protected with strong encryption. If the PAN is not stored, this requirement is lifted.

Sensitive information is security-related information. This includes (but is not limited to) card validation values (CVV), full track data (from the magnetic stripe or equivalent on a chip), PINs and PIN blocks. This information is used to authenticate cardholders and/or authorise payment card transactions.

Under no circumstances can sensitive information be stored in any form after authorisation.

Permitted Use of Card Data

ICAEW will accept payments by card using approved point-of-sale (POS) devices, phone and our website using approved processes only. Any other mechanisms for accepting card payments are expressly prohibited.

ICAEW will not store payment card data in any form (including voice recordings, emails or screen captures) and will not transmit card payment data. Where card payments are taken, these capabilities are to be handled by external 'service providers' who must be certified as being PCI DSS compliant. ICAEW will only use approved devices and service providers to perform these tasks.

It is therefore mandatory throughout ICAEW that no new projects, software development, business initiatives, support activities, mergers or acquisitions put ICAEW in a position where we would need to store payment card data, and/or process and transmit card payments in any form without using a PCI DSS certified external service provider.

Please review to the PCI DSS Policy for further information.

Compliance

PCI-DSS Compliance also requires ICAEW to complete a self-assessment questionnaire on an annual basis, supported by IT related security scans of ICAEW infrastructure on a regular basis.

Non-compliance with this policy should be reported to the <Responsible Individual>.

Review of security policy and technical compliance

Objective: To ensure compliance of systems with organisational security policies and standards.

Compliance with security policy

ITD shall audit compliance with this policy document. All line managers shall ensure that staff within their area of responsibility complies with this policy document.

Technical compliance checking

Technical compliance checking involves the examination of operational systems to ensure that hardware and software controls have been correctly implemented. The ITD Security Team shall therefore conduct periodic checks of information systems for compliance with security implementation standards. This could also include the ITD Infrastructure where identified.

System audit considerations

Objective: To maximise the effectiveness, and to minimise interference to/from the system audit process.

System audit controls

System audit shall be conducted at least annually or on significant change of IT provision. Audit requirements should be documented in accordance with current procedures.

Protection of system audit tools

The operating systems provide security access to the auditing tools. However, the ITD Security Team shall conduct regular checks of the audit log for signs of tampering/ unauthorised access. Other third party tools are to be secured and access restricted.

APPENDIX A SECURITY CONSIDERATIONS IN OUTSOURCING CONTRACTS

This use of all cloud-based web services require the signoff for use from either the IT Director or the IT Security Manager prior to going live.

For further advice please contact the IT Security Manager.

The security items which need to be included (this list is not exhaustive) are as follows:

The security items to be included (this list is not exhaustive) are as follows:

- The general policy on information security
- Asset protection including:
  - Procedures regarding protection of organisational assets, including information and software
  - procedures to determine whether any compromise of the assets, e.g. loss or modification of data has occurred
  - Controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the contract
  - Data integrity and availability
  - Restrictions on copying and disclosure information
- A description of each service to be made available
- The target level of service and unacceptable levels of service
- Provision for the transfer of staff where appropriate
- The respective liabilities of the parties to the agreement
- Responsibilities with respect to legal matters
- Intellectual property rights and copyright assignment and protection of any collaborative work
- Access control agreements, covering
  - permitted access methods, and the control and use of unique identifiers such as user IDs and passwords
  - an authorisation process for user access and privileges
  - a requirement to maintain a list of individuals authorised to use the services being made available and what their rights and privileges are with respect to such use
- The definition of verifiable performance criteria, their monitoring and performance
- The right to monitor, and revoke, user activity
- The right to audit contractual responsibilities
- The escalation process for outstanding issues; contingency arrangements should be considered where appropriate
- Responsibilities regarding hardware and software installation and maintenance
- A clear reporting structure and agreed reporting formats
- A clear and specified process of change management
- Any required physical protection controls and mechanisms to ensure those controls are followed
- User and administrator training in methods, procedures and security
- Controls to ensure protection against the spread of computer viruses

- Arrangements for joint reporting, notification and investigation of security incidents and security breaches
- Involvement of the third party with sub-contractors
- How the legal requirements are met (e.g. data protection legislation)
- What arrangements will be in place to ensure that all parties involved in the outsourcing are aware of their security responsibilities
- How the confidentiality of the organisation's sensitive business information is to be maintained
- What physical and logical controls will be used to restrict and limit the access to the organisation's sensitive business information to authorised users
- How the availability of services is to be maintained in the event of a disaster
- What levels of physical security are to be provided for outsourced equipment

APPENDIX B PRÉCIS OF IT SECURITY LEGISLATION

The information below is intended simply as a basic guide to existing legislation with direct regard to IT security, and should not be taken as complete and authoritative legal advice.

The key points of this legislation are as follows:
A person commits an offence under the CMA 1990 if:

1. He/she causes a computer to perform any function with intent to secure access to any program or data held in any computer
2. The access he/she intends to secure is unauthorised
3. He/she knows at the time when he/she causes the computer to perform this function that this is the case.

Intent to commit an offence under the act need not be directed at:

a) Any particular program or data
b) A program or data of any particular kind
c) A program or data held in any particular computer.

A person found guilty of such offences may be liable to summary conviction to imprisonment for a term not exceeding six months, or to a fine, or both.

With a few exceptions, any data controller who holds personal information must register with the Data Protection Commissioner. Personal data, in this instance, is defined as information which identifies an individual. When the data controller registers an entry, the following information must be supplied:

a) The data controller's name
b) The data controller's address
c) A description of the data to be stored
d) The purposes for which the data is to be used
e) The people and entities to which the data controller may wish to supply the data in question
f) Any overseas country to which the data controller may wish to supply the personal data
g) General description of the security measures taken to protect the data.

Eight data protection principles exist, to which the data controller must then comply. These state that any personal data held by the data controller shall:

1. Be obtained and processed fairly, transparently and lawfully
2. Be held and processed only for the lawful purposes described in the register entry
3. Be held only for those purposes and only be disclosed for those to those people in the register entry
4. Be adequate, relevant, and not excessive in relation to the purpose for which they are held
5. Be accurate, and where necessary, kept up to date
6. Be held no longer than is necessary for the registered purpose
7. Be surrounded by adequate security
8. Be accountable for, and be able to demonstrate compliance with the other principles.

In addition, the data controller shall not transfer data out of the UK unless adequate safeguards are established in line with the relevant data protection law.
Offences under the DPA 1998 are punishable by a fine of £20million or 4% of revenue.

These Acts cover fraudulent or improper use of telecommunications systems, and by extension, other services operating across telecommunications systems, e.g. electronic communications. Key offences under these Acts include:

- Dishonestly obtaining goods or services
- Avoiding payment for goods or services
- Sending messages or other matter that is offensive , indecent, obscene, or menacing in character
- Sending messages or other material intended to annoy, cause inconvenience, or cause needless anxiety
- Sending a message or other material known to be false, or persistently making use of telecommunications systems for that purpose.

Offences are punishable by imprisonment for up to two years, or a fine up to the statutory maximum, or both.

The main purpose of the Act is to ensure that the relevant investigatory powers are used in accordance with human rights. These powers are:

- the interception of communications;
- the acquisition of communications data;
- intrusive surveillance;
- covert surveillance in the course of specific operations;
- the use of covert human intelligence sources;
- Access to encrypted data.

For each of these powers, the Act will ensure that the law clearly covers:
The purposes for which they may be used;

- which authorities can use the powers;
- who should authorise each use of the power;
- the use that can be made of the material gained;
- independent judicial oversight;
- A means of redress for the individual.

The Act will work in conjunction with existing legislation, in particular the Human Rights Act 1998.

This Act gives further effect in the UK to the fundamental rights and freedoms in the European Convention on Human Rights. The basic rights within the Act do not only affect matters of life and death like freedom from torture and killing; they also affect your rights in everyday life i.e. what you can say and do, your beliefs, your right to a fair trial and many other similar basic rights.

Other IT legislation may have direct bearing on ICAEW operations, if particular developments take place. For example, adoption of digital signatures will mean that the Electronic Communications Act 2000 has relevance.

APPENDIX C GLOSSARY OF SECURITY TERMS

TERM	MEANING
Access Control	The process of ensuring that systems are only accessed by those authorised to do so, and only in a manner for which they have been authorised.
Access Model	A type of security model, which represents a secure system in terms of subjects (active processes), objects (passive containers of information), and access modes (e.g. read, write, execute).
Application Layer	The Layer of the OSI Reference Model which provides communication between applications
Application Security	The provision of security services at the Applications Layer of the OSI model
Audit Trail	An audit trail may be on paper or on electronic media. In computer security systems, a chronological record of security-relevant events e.g. when users log in, how long they are engaged in various activities, what they were doing, whether any actual or attempted security violations occur.
Authentication	The verification of a claimed identity.
Availability	The prevention of unauthorised withholding of information or resources.
Back Door	An undocumented means of bypassing the normal access control procedures of a computer system.
Confidentiality	The process of ensuring that data is not disclosed to those not authorised to see it.
Contingency Planning	Preparing for any possible eventuality which will have effect on the availability of a system or service.
Countermeasure	A mechanism that reduces the vulnerability to a threat to a system.
Denial of Service	Reduction of the availability of a resource below the level needed to support critical processing or communication requirements.
Digital Signature	A means of protecting a message from denial of origination by the sender, usually involving the use of asymmetric encryption to produce an encrypted message or a cryptographic checksum. Can also be used to provide message integrity.
Encryption	The general term for hiding information in secret code or cipher.
Firewall	A system or combination of systems that enforces a boundary between two or more network and mediates network traffic on the basis of a security policy.
Gateway	A device connecting two networks.
Hacking	Unauthorised use or attempts to circumvent or bypass the security mechanisms of an information system or network. Hacking can be either internal or external.
Integrity	A security protection aimed at ensuring that data cannot be deleted, modified, duplicated or forged without detection.
Intrusion Detection	Detection of break-ins or break-in attempts either manually or via software expert systems that operate on logs or other information available on the network.
Key	The general concept of protecting things with a "lock," thus making those things available only if one has the correct "key."

TERM	MEANING
	In cryptography we have various kinds of keys, including a User Key (the key which a user actually remembers), which may be the same as an Alias Key (the key for an alias file which relates correspondent names with their individual keys). We may also have an Individual Key (the key actually used for a particular correspondent); a Message Key (normally a random value which differs for each and every message); a Running Key (the confusion sequence in a stream cipher, normally produced by a random number generator); and perhaps other forms of key as well.
Key Management	The process of securely generating, transporting, storing, revoking and destroying encryption keys.
Least Privilege	Designing operational aspects of a system to operate with a minimum amount of system privilege. This reduces the authorisation level at which various actions are performed and decreases the chance that a process or user with high privileges may be caused to perform unauthorised activity resulting in a security breach.
Message Authentication	Assurance that a message has not been modified in transit or storage. Can be achieved with cryptography.
Non repudiation	Establishing a property by a message or transaction that with high assurance can be asserted to be true, and not subsequently refuted. Examples are non-repudiation of origin (an authentication property) and non-repudiation of delivery (of a message).
Risk	The combination of the likelihood that vulnerability may be exploited and the adverse impact of that event.
Risk Analysis	The analysis of a system's assets, threats and vulnerabilities in an attempt to establish the expected adverse impact when a given incident occurs. Having identified a risk, the options are to accept the risk, apply measures to reduce the risk to an acceptable level, or transfer the risk to another party.
Risk Assessment	The process of assessing the level of security risk of a system.
Risk Management	The process of minimising total risk.
Security	Protection against unwanted behaviour or events. The most widely used definition of computer security is security = confidentiality + integrity + availability. In business an additional objective is revenue protection.
Security Model	A set of precise rules describing how security may be represented and upheld in a computer system. A security model may be system-specific, being derived from a system-specific security policy, or may be generic, derived from a general security policy.
Security Policy	A security policy is the set of high-level rules, principles and practices that determine how security is implemented in an organisation.
Separation of Concerns	A principle of design that separates functions of differing security or integrity into separate protection domains. Separation of concerns is sometimes implemented as an authorisation rule in which two or more subjects are required to authorise an operation.
System High	Where security is defined at the system level; i.e. all users of the system have the same security clearance.

TERM	MEANING
Tamper Resistance	The property in data security equipment that provides facilities for detecting attempts to tamper with the equipment, and may detect such attempts and ensure that an appropriate response is made.
Threat Assessment	Evaluating all of the possible threats that can be made against a computer system.
Token	A "token" is typically an authentication device utilised to send and receive challenges and responses or generates one-time passwords during the user authentication process. Tokens may be small, hand-held hardware devices similar to pocket calculators or credit cards. Smart Cards are used as authentication tokens also.
Trojan Horse	A computer program whose execution would result in undesired side effects, generally unanticipated by the user. The Trojan Horse program may otherwise give the appearance of providing normal functionality.
Virus	A program which makes copies of itself in such a way as to 'infect' parts of the operating system and/or application programs.

APPENDIX D CONFIDENTIALITY STATEMENT

The purpose of this confidentiality statement is to ensure all staff, whether permanent, temporary or contractors understand their responsibility for confidentiality of information. The following general rules apply.

All staff should acknowledge that in the course of performing work for ICAEW they will have access to information held by ICAEW and all such information should be regarded as confidential. The confidential information should only be used in the course of and exclusively for the purposes of performing work for ICAEW and this obligation of confidentiality will survive termination of any work engagement with ICAEW.

Other than in the proper course of performing duties for ICAEW, confidential information should not be divulged to the Press or anybody outside ICAEW.

Upon termination of any work engagement with ICAEW, all tangible copies of ICAEW confidential information and all ICAEW property should be returned, unless written consent has been given by ICAEW to retain items.

All staff should be aware that work produced during the course of employment with ICAEW, becomes the property of ICAEW.

Intellectual Property means inventions, designs, discoveries, processes, formulae, trade secrets, research and development information, preparatory designs, design standards, specifications, notations, improvements, know-how, goodwill, reputation, get-up, trade names and marks, internet domain names or similar electronic identifiers, logos, devices, plans, models, drawings, technical, functional or user documentation, computer software (including source code and object code), data, databases, all descriptions of work in which copyright subsists as set out in the Copyright Designs and Patents Act 1988 (including without limitation all literary, dramatic, musical and artistic works) and all other related matters.

All staff will not at any time remove any equipment or software or related documentation from ICAEW premises without express prior written permission from ICAEW. In the event such permission is given, the member of staff agrees to be fully responsible for the safe custody and security of such equipment or software or documentation.

All staff should undertake to observe all reasonable instructions and directions of ICAEW including but not limited to the nature of the task to be performed, information security instructions, data protection guidelines and health & safety and administrative procedures.

If, in the course of your work, you are responsible for considering any matter where your objectivity might be called into question because of any relationship you may have with any individual e.g. husband, wife, relative, friend, past employer, firm or organisation, you should immediately report this to your manager so that consideration can be given as to whether the task should be reallocated to another member of staff.

Document control

Date: March 2024
Expiry: March 2025
Confidentiality: ICAEW use only
Version: 6.0
Owner: Bill Wilson
Drafted by: Jason Harris
Approved by: Director, IT & Property
Next review date: February 2025
Linked documents: IT Security User Guide
Payment Card Industry Data Security standard (PCI DSS)
Data Protection Policy
Social media Policy
Data Management Policy
Bring Your Own Device Policy (BYOD)
Electronic Communications Monitoring Policy