5 E Ltd
Selby Centre
Selby Road
London N17 8JL
Tel: 020 8885 3456
Fax: 020 8808 9977
Email: enquiries@fivee.co.uk
Website: www.fivee.co.uk

Information Security Policy

1. Introduction

1.1 Background

This Information Security Policy has been compiled jointly by 5 E Ltd *(herein after referred to as the organisation)* and its partner organisations. It is based upon the International Standard ISO 27001 & 27002, the Code of Practice for Information Security Management, which contains comprehensive sets of security controls to improve the level of security within the organisation.

1.2 Requirements for Policy

The organisation has an obligation to its members to clearly define requirements for the use of its information technology (IT) facilities and its information systems (IS). This is so that users of IT/IS facilities do not unintentionally place themselves, or the organisation, at risk of prosecution, by carrying out computer related activities outside the law.

In addition, although the bulk of information at the organisation is intended to be openly accessible and available for sharing, certain information (key data and information) has to be processed, handled and managed securely and with accountability. Legislation is again the key driver of this requirement, but it is also derived from the criticality and sensitivity of certain information where loss of accuracy, completeness or availability could prevent the organisation from functioning efficiently, or where disclosure could damage the organisation's reputation. Unless policy is in place to stipulate control requirements for such information, there is an increased risk that security breaches will be suffered, potentially resulting in a wide-range of adverse consequences.

1.3 Policy Structure

This document forms the organisation's Information Security Management System Policy (henceforth referred to as The Policy). Its purpose is to provide an overarching framework (a commitment of undertaking) to apply information security controls throughout the organisation.

Supporting Policies containing detailed Information Security requirements will be developed in support of The Policy. Dependent upon the subject matter, Supporting Information Security Policy

Policies will apply either holistically or to specific groups or individuals within the organisation. Members of the organisation, who have access to the organisation's computers, information systems and key information, and all other parties who have been granted such access, are responsible for complying with Supporting Policies that are applicable to them.

Reference to Supporting Policies is made in bold italic text throughout the remainder of the document.

1.4 Purpose and Scope

Information plays a major role in supporting the organisation's academic, vocational and administrative activities. The purpose of The Policy is to provide a framework for protecting:

- The organisation 's IT/IS infrastructure;
- Key data and information;

- Those who have access to or who administer IT/IS facilities;
- Individuals who process or handle key data and information.
- The Policy is designed to provide protection from internal and external security
- threats, whether deliberate or accidental by:
- Defining The organisation 's policy for the protection of the Confidentiality,
- Integrity and Availability of its' key data and information;
- Establishing responsibilities for information security;
- Providing reference to documentation that comprises the Information Security Management System (ISMS).

  In doing so, The Policy supports the organisation's Electronic Security, Data Backup and Recovery Policy Statement and Electronic Security, Data Backup and Recovery Policy Guidelines. The organisation's members will also derived benefit from applying the requirements of this policy for the protection of non-key data if they should so wish.

1.5 Objective

Information Security controls are designed to protect members of the organisation and the organisation's reputation through the preservation of CIA (Confidentiality, Integrity and Availability):

- Confidentiality - knowing that key data and information can be accessed only
- by those authorised to do so;
- Integrity - knowing that key data and information is accurate and up-to-date,
- and has not been deliberately or inadvertently modified from a previously
- approved version; and,
- Availability - knowing that the key data and information can always be accessed.

The organisation is committed to protect both its members and its key data and information and to deploy controls that minimise the impact of any Security Incidents.

1.6 Applicability

The Policy applies to the following categories, referred to hereafter as 'subjects'.

- All full-time, part-time and temporary staff employed by, or working for or
- on behalf of The organisation ;
- Students studying at The organisation ;
- Contractors and consultants working for or on behalf of The organisation ;
- All other individuals and groups who have been granted access to The Organization's IS/IT systems and/or key data and information.

The Director, Chief Information Security Officer (CISO), Information Security Manager (ISM), Centre Managers and Policy & Compliance Team are ultimately responsible for ensuring that the Policy is implemented within their respective Satellite Centres and for overseeing compliance by subjects under their direction, control or supervision.

It is the personal responsibility of each person to whom The Policy applies to adhere with its requirements.

2. Organisational Security

Information security governance will be implemented to ensure effective controls are in place throughout the organisation.

2.1 Information Security Infrastructure

An Information Security Infrastructure will be developed to support the Policy.

2.1.1 Ownership and Maintenance of the Policy

The organisation's Director chaired by Director is committed to the company's Information Security Policy. Security Committee chaired by the Chief Security Officer maintains the policy with Information Security Manager and include representatives from administrative departments, service departments, utilising specialist input where contents or topics warrant this.

2.1.2 Review

An independent review of the implementation of The Policy, its effectiveness and the degree of compliance with it will be carried out periodically by Information Security Manager.

2.2 Security of Third Party Access

Access to The organisation's information processing facilities by third parties will be controlled.

2.2.1 Identification of Risks from Third Party Access

Third parties who require access to the organisation's IT/IS infrastructure will be bound by a contract that defines organisation security requirements. Prior to being granted any network connectivity they will be required to sign an undertaking to adhere to the requirements of the Third Party Access Policy and where key data is involved, they will be required to sign a non-disclosure agreement.

3. Asset Classification

Information assets will be categorised and recorded to enable appropriate management and control.

3.1 Inventory of Assets

Inventories of information assets, including hardware, software and key data will be developed and maintained in accordance with the Asset Management Policy.

3.2 Protection of Key Data and Information

Key data and information will be classified, protectively marked and handled and managed in accordance with the Information Classification Policy.

4. Personnel Security

Controls will be deployed to reduce the risks of human error, theft, fraud, nuisance or malicious misuse of facilities within the organisation.

4.1 Security in Job Descriptions

Security roles and responsibilities will be included in job descriptions 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 Personnel Screening Policy

Steps will be taken in accordance with the Personnel Security Policy to minimise the likelihood of personnel, who pose a security risk, being employed in posts involving key data and information, such as those concerned with financial or personnel related data.

4.2.1 Confidentiality Undertaking

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

4.2.2 Employee Responsibilities

Employees will informed of their information security responsibilities during induction training and these will be reiterated on appropriate organisation websites in accordance with the Information Security Awareness & Training Policy.

4.3 Education and Training

4.3.1 Information Security Education and Training

Information security awareness training and / or instruction will be made available to staff. The Information Security Awareness & Training Policy will identify where such training is mandatory.

Customers and other users, such as visitors, maintenance etc. and other third parties, will be made aware of their responsibilities through various information security awareness documents and publications.

4.4 Responding to Security Incidents

4.4.1 Suspected Security Weaknesses

Those subjects using or administering the IT/IS facilities must not try and prove any suspected or perceived security weakness. The exception to this rule is where support staff have been granted a specific policy exemption which allows them to do so as part of their role.

4.4.2 Reporting Security Incidents

All actual and suspected security incidents are to be reported to the Prime Contractor and/or Department for Works and Pensions.

4.4.3 Network Isolation and Reconnection

Any computer that is perceived to be placing the integrity of the campus network at risk will be disconnected at the organisation's network boundary in accordance with the Access Control Policy. Subsequent reinstatement will only be permitted once the requirements of that policy have been met.

4.4.5 Security Incident Management

Events that are regarded as being 'security incidents' will be defined, and processes implemented to investigate, control, manage and review, with a view to preventing recurrence.

The organisation is to develop and maintain a Critical Incident Management Plan and Business Continuity Strategy for implementation in the event of any major security incident that occurs.

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

Computer systems and networks will be protected by suitable physical, technical, procedural and environmental security controls in accordance with the Physical Security & Access Control Policy.

File servers and machines that hold or process high criticality, high sensitivity or high availability data will be located in physically secured areas.

Access to facilities that hold or process high criticality, high sensitivity or high availability data (as defined with the Information Classification) will be controlled.

5.2 Office Security

Key Information will be protected in accordance with the Information Classification Policy.

6. Communication and Operations Management

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

6.1 Documented Operating Procedures

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. IT/IS operating procedures shall be documented and maintained.

6.2 Segregation of Duties

Access to critical systems and key data and information will only be granted on a need to know basis. Segregation of duties between operations and development environment shall be maintained for critical systems. Permanent and full access to live operating environments will be restricted to staff on role-based requirements. Sensitive operations will be identified and action taken to implement split functional controls where appropriate.

6.3 Systems Planning and Acceptance

6.3.1 Capacity Planning

Appropriate processes and procedures will be implemented in respect of capacity planning and alerting for critical systems as defined in the Information Classification Policy.

6.3.2 System Changes

All changes to live critical systems will follow a pre-defined change management process, to ensure that activities are undertaken in accordance with

stringent change control process in accordance with the Change Control Policy.

6.3.3 Security Assurance Testing

Critical systems, as defined by the Information Classification Policy, will be subjected to periodic security assurance testing in accordance with the Security Assurance Testing Policy.

6.4 Controls against Malicious Software

Controls will be implemented to check for malicious or fraudulent code being introduced to critical systems. Source code written by contractors and staff will be subjected to security scrutiny before being installed on any live critical system.

6.5 Security Patches, Fixes and Workarounds

Member of The organisation who are responsible for the day to day management of systems are to ensure that security patches, fixes and workarounds are applied.

6.6 Housekeeping

6.7.1. Data Storage

Data on critical systems will be managed in accordance with the Backup Strategy and Disaster Recovery Policy.

6.7.2 System, Application and Data Backup

All critical systems, applications and key data will be backed up in accordance with the Backup Strategy and Disaster Recovery Policy.

6.7.3 Archiving

All archive material will be held, managed and stored in accordance with the Documentation Retention Policy.

6.8 Network Management

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

6.9 Media Handling and Security

6.9.1 Handling and Storage

Media containing key data will be marked and handled in accordance with the Information Classification Policy and managed in accordance with the Backup Strategy and Disaster Recovery Policy.

6.9.2 Disposal

Removable magnetic and optical media containing key data will be reused or disposed of through controlled and secure means when no longer required, in accordance with the Information Classification Policy.

Procedures will be made available in accordance with the Information Classification Policy for the secure disposal of disk drives and disk packs containing key data when these become defunct or unserviceable.

Where custody of equipment containing key data is to be relinquished, procedures will be implemented in accordance with the Information Classification Policy to securely delete such data first.

Redundant computer equipment will be disposed of in accordance with the Waste Electrical and Electronic (WEEE) Regulations and through secure and auditable means.

6.10 Exchanges of Information and Software

6.10.1 Software Usage and Control

Software will be used, managed and controlled in accordance with legislative requirements and the ICT Usage policy.

All major software upgrades and in-house systems development for critical systems will be appropriately controlled and tested through a managed process before live implementation, as defined in the Information Classification Policy.

6.10.2 Internet Usage

Activities involving Internet usage, for example e-mail transmission and web site access, will be governed by the ICT Usage policy.

Systems that provide any external service, such as web and e-mail servers, must be registered with ISS to enable any security notifications to be passed on to those responsible for their maintenance.

7. Access Control

Access to key data and information will be appropriately controlled.

7.1 User Responsibilities

Subjects who use the organisation's computer systems and/or networks must do so in accordance with the ICT Usage policy.

7.2 organisation Requirements for Systems Access

7.2.1 Access Management and Administration

Authorised access to the organisation's Information Systems facilities in accordance with specific privileges that they have been given. Formal procedures will be implemented for granting access to organisation's Information Systems Secure ISMS systems, for all users. This will be supported by a formal review of user privileges on a regular basis to ensure that they remain appropriate, and dormant accounts will be closed in accordance with the Access Control Policy.

7.2.2 Remote Access

Controls will be implemented to manage and control remote access to the organisation's ISMS and key data.

7.2.3 Privilege Management

The allocation and use of system privileges on each computer platform shall be restricted and controlled in accordance with the Access Control Policy.

7.2.4 Password Management

The allocation and management of passwords shall be controlled in accordance with the Password Policy.

7.2.5 Passwords

Users are required to follow good security practices in the selection, use and management of their passwords and to keep them confidential in accordance with the Password Policy.

7.2.6 Unattended User Equipment

Users of ISMS are responsible for safeguarding key data by ensuring that desktop machines are not left logged-on when unattended, and that portable equipment in their custody is not exposed to opportunistic theft.

Where available, password protected screen-savers and automatic log-out mechanisms are to be used on office based systems to prevent individual accounts being used by persons other than the account holders, but not on cluster computers that are shared by multiple users.

7.3 Network Access Control

The use of networked services, connectivity to the organisation network and the use of information systems connected to the organisation network.

7.4 Operating System and Application Access Control Access to systems' operating systems and applications will be controlled in accordance with the Access Control Policy. System utilities software will be held securely when not in use and access will be strictly restricted to authorised staff.

7.5 Monitoring System Access and Use

Access to and use of critical systems will be monitored in accordance with the ICT Usage Policy

8. Systems Development and Maintenance

Controls will be implemented to ensure that security requirements are considered when developing existing information systems and prior to introducing new ones.

8.1 Security Requirements within Projects

Project Managers are to undertake a risk assessment, in accordance with the Risk Assessment Policy, to identify security requirements for new organisation systems.

8.2 Use of Cryptography

System administration and account management passwords will be encrypted at all times. The use of all cryptographic controls will be in accordance with the Cryptographic Usage Policy.

8.3 Security in Test and Development Processes

Test and development systems will be appropriately isolated from live critical systems at all times.

9. Business Continuity Management

Controls will be implemented to counteract disruptions to the organisation's information processing facilities and to protect critical systems from the effects of major failures and disruption.

9. Data Storage

Ideally, key data will be held on a network resource so that it is backed up through a routine managed process. Where this is not possible, provision must be made for regular and frequent backups to be taken in accordance with the Information Classification & Protection Policy and the Data Backup & Storage Policy.

9.2 Backup Media

A controlled and fully auditable process for the handling, transportation, storage and retrieval of backup media containing key data will be implemented.

9.3 Business Continuity Management

A Business Continuity strategy will be developed, exercised and maintained to ensure the availability of services in the event of unexpected disruption in accordance with the Business Continuity Policy.

10. Compliance

Controls will be implemented to avoid contravention of legislation, regulatory and contractual obligations and security policy.

10.1 Legal Requirements Policy

Legislation that has a bearing on information processing and management will be identified and controls will be implemented to ensure compliance in accordance with the Legal Requirements Policy.

10.2 Review of Security Policy

The Policy will be subjected to review annually and in the event of any major changes in circumstances, to ensure those controls remain effective. In addition, anyone wishing to raise a policy change request may complete by a formal request made to the Information Security Manager.

10.3 Compliance with Security Policy

Compliance with The Policy is mandatory. Failure to comply with policy requirements, outside the process for exemption authorisation, will be viewed as a breach of security. Any such event may be the subject of investigation and possible further action in accordance with organisation procedures. Senior Management Team, along with Centre Managers shall ensure that security policy is adhered to within their departments and throughout the organisation. All parts of the organisation will be subject to review to ensure compliance with the policy.

10.4 Exemptions

In certain circumstances it may not be practical for some subjects or functional departments to rigorously adhere to specific areas of The Policy. Where there are justifiable reasons why a particular policy requirement cannot be implemented, a specific policy exemption must be requested.

Review

This was reviewed in June 2018 and is due for next review in June 2019.

If you require this policy in a larger font size, please contact the HR Department.