



FORTHS FORENSIC ACCOUNTANTS

INFORMATION SECURITY POLICY

Introduction

Forths Forensic Accountants, like other organisations, relies on information to fulfil its aims, objectives and obligations. Information, and the systems which support it, are vitally important Forths Forensic assets. Their availability, integrity, security and confidentiality are essential to maintain service levels, compliance and image of Forths Forensics.

Effective Information Security will help to control and secure information from inadvertent or malicious changes and deletions or unauthorised disclosure.

Policy Objectives

The objectives of the Information Security Policy of Forths Forensics are to ensure that:

- All employees are aware of the policy statement and associated legal and regulatory requirements and of their rights and responsibilities in relation to Information Security
- All Forths Forensic assets, including equipment and data, are adequately protected
- A high level of awareness exists of the need to comply with Information Security measures
- Where appropriate, monitoring arrangements are put in place ensure compliance with policy objectives, guidelines and standards
- The Information Security Policy and associates papers are reviewed regularly

Policy Scope

The Information Security Policy applies to:

- All employees of Forths Forensics
- All employees and agents of external organisations who in any way support or access any Forths Forensic information system.

And information which is:

- Shared on computers
- Transmitted across networks
- Printed out
- Written on paper
- Sent by fax
- Stored on tapes or disks
- Spoken in conversation, e.g. by telephone
- Sent via e-mail
- Stored on databases

Aims of Information Security

The aims of Information Security are to:

- Ensure that business continuity is maintained and damage to business is minimised by the impact and incidence of security incidents
- Ensure that legislative and regulatory requirements are met in respect of information and data security.

Revision of Information Security

The Information Security Policy and associated guidelines for specific areas of Information Security will be developed by the Directors of Forths Forensics and agreed and implemented by the same.

The remit shall include:

- The development of the Information Security Policy and its associated papers

- The implementation of the policy and guidelines through training and awareness
- The development and implementation of standards and procedures outlined in the papers
- Compliance with the policy and guidelines.

Security Incidents

A security incident can be defined as an event that has, or could have, resulted in loss or damage to Forths Forensic assets, or an event which is in breach of Forth Forensic security procedures.

All employees have a responsibility to report security incidents as quickly as possible through the defined channel. This obligation also extends to employees and agents of external organisations contracted to support or access the Information Systems of Forths Forensics.

Standard procedures will be defined for reporting and investigation these incidents in the associated policy documents.

Principles of Information Security

The Information Security Policy is based on the 10 principles set out in ISO 17799, the British Standard for Information Security.

- 1 Security Policy
- 2 System Access Control
- 3 Computer & Operations Management
- 4 System Development and Maintenance
- 5 Physical and Environmental Security
- 6 Compliance
- 7 Personnel Security
- 8 Security Organisation
- 9 Asset Classification and Control
- 10 Business Continuity Management (BCM)

1 Security Policy

The objective of this principle is to provide management direction and support for information security. The policy development and review process will focus on:

- 1) The frequency and impact of security incidents.
- 2) Compliance with Council policy.
- 3) Changes in relevant legislation e.g. changes precipitated by cases involving Human Rights legislation.

- 4) Changes in working policy or practice.
- 5) Training needs.

To meet the objective:

- Supplementary guidelines will be produced as necessary.

2 System Access Control

The objectives of this principle are to:

- 1) Control access to information
- 2) Prevent unauthorised access to information systems
- 3) Ensure the protection of networked services
- 4) Prevent unauthorised computer access
- 5) Detect unauthorised activities
- 6) Ensure information security when using mobile computing and tele-networking facilities

To meet these objectives:

- Acceptable Use Guidelines have been put in place for E-mail and Internet use. These guidelines will be reviewed regularly and updated as necessary to comply with changing legislation and Forth's Forensics policy
- All Forth's Forensic provided Internet access is filtered to reduce the risk of illegal or inappropriate material being accessed
- Access to areas where information is stored e.g. the computer room and records management area is controlled, and is limited to only those who need to be there
- Access to systems must be authorised by appropriate Directors.

3 Computer & Operations Management

The objects of this principle are to:

- 1) Ensure the correct and secure operation of information processing facilities
- 2) Minimise the risk of systems failures
- 3) Protect the integrity of software and information
- 4) Maintain the integrity and availability of information processing and communication
- 5) Ensure the safeguarding of information in networks and the protection of the supporting infrastructure
- 6) Prevent damage to assets and interruptions to business activities

- 7) Prevent loss, modification or misuse of information exchanged between organisations.

To meet these objectives:

- Backups of data from major systems are held both on and off site
- Network traffic is monitored daily

4 Systems Development and Maintenance

The objectives of this principle are to:

- 1) Ensure security is built into operational systems
- 2) Prevent loss, modification or misuse of data
- 3) Protect the confidentiality, authenticity and integrity of information
- 4) Ensure IT projects and support activities are conducted in a secure manner
- 5) Maintain the security of application system software and data

To meet these objectives:

- Security measure (e.g. password controls, data validation, backup processes) are built into systems as they are developed and implemented
- Security management guidelines will be produced and issued to all Services. These guidelines will specify procedures for identifying and dealing with security incidents
- Security issues relating to the development, testing and implementation of systems will be identified and addressed.

5 Physical and Environmental Security

The objectives of this principle are to:

- 1) Prevent unauthorized access, damage and interference to business premises and information
- 2) Prevent loss, damage or compromise of assets and interruption to business activities
- 3) Prevent compromise or theft of information and information processing facilities.

To meet these objectives:

- Fire Extinguishers are in operation in the computer room

- Access to the records management file store is restricted
- Servers are kept in 'safe' areas, either in locked rooms or in supervised work areas
- Backups are held in secure storage

6 Compliance

The objectives of this principle are to:

- 1) Avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements
- 2) Ensure compliance of systems with organizational security policies and standards
- 3) Maximise the effectiveness of and to minimize interference to/from the system audit process

To meet these objectives:

- Forth's Forensic undertakes to comply with all relevant legislation (e.g. Data Protection Act, Computer Misuse Act, Regulation of Investigatory Powers Act, Human Rights Act, Copyright, Design and Patents Act, Freedom of Information Act).

7 Personnel Security

The objectives of this principle are to:

- 1) Reduce risks of human error, theft, fraud or misuse of facilities
- 2) Ensure that users are aware of information security threats and concerns, and are equipped to support the corporate Information Security Policy in the course of their normal work
- 3) Minimise the damage from security incidents and malfunctions and learn from such incidents.

To meet these objectives:

- Training is offered to all computer users. Training ranges from basic 'Introduction to Computers' to advanced use of standard software depending on the requirements of the individual
- Staff are advised not to divulge their passwords
- Backups are carried out regularly and stored safely

- Guidelines have been developed relating to personal use of Forths Forensic computer equipment
- Guidelines have been developed relating to the removal of laptops and paper files outwith the business premises
- Guidelines have been developed relating to identifying and notifying security incidents

8 Security Organisation

The objectives of this principle are to:

- 1) Manage Information Security within the organisation
- 2) Maintain the security of organisational information processing facilities and information assets accessed by third parties
- 3) Maintain the security of information when the responsibility for information processing has been outsourced to another organisation

To meet these objectives:

- Advice and guidance on all aspects of Information Security shall be given
- Dial-up connection to the Forths Forensic network is only allowed under strictly controlled conditions

9 Asset Classification and Control

The objectives of this principle are to:

- 1) Maintain appropriate protection of corporate assets
- 2) Ensure that information assets receive an appropriate level of protection

To meet these objectives:

- An asset register of all equipment is kept. This register must be reviewed and, where necessary, updated by all Services annually
- A register is kept of all software installed on Forths Forensic computers.

10 Business Continuity Management (BCM)

The objective of this principle is to protect business activities and critical business processes from the effects of major failures or disasters. To meet this objective:

Summary

The purpose of this policy is to protect the information assets of Forths Forensics from all internal, external, accidental or deliberate threats.

The Information Security Policy will ensure that:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Information will be processed accurately
- Regulatory and legislative requirements will be met
- Information Security training and material will be available to all employees and Elected Members
- All security breaches will be reported and investigated in the defined manner
- Business Continuity plans will be produced, tested and maintained