
INFORMATION SECURITY POLICY

The Board and management of Forth Communication NI Ltd, located at Units 1A, 2B, 3C, 32 IT Centre, 2-4 Balloo Avenue, which undertakes Data Processing & enhancement, Website development, document imaging and mailing project management services, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout Forth Communication in order to preserve its competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image. Information and information security requirements will continue to be aligned with Forth Communication goals and the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations, and for reducing information-related risks to acceptable levels.

Forth Communication's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS. The risk assessment, Statement of Applicability and risk treatment plan identify how information-related risks are controlled. The Managing Director is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

In particular, business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in the Manual and are supported by specific, documented policies and procedures.

All employees of Forth Communication and certain external parties identified in the ISMS are expected to comply with this policy and with the ISMS that implements this policy. All staff, and certain external parties, will receive or be required to provide appropriate training.

The ISMS is subject to continuous, systematic review and improvement.

Forth Communication has established a top level management steering group, chaired by the Managing Director and including the Information Security Manager and other executives to support the ISMS framework and to periodically review the security policy.

Forth Communication NI Ltd is committed to maintaining certification to ISO 27001:2005.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan and at least annually.

INFORMATION SECURITY POLICY

In this policy, “information security” is defined as:

Preserving

This means that management, all full time or part time staff, sub contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches (in line with the policy and procedures identified in section 13 of the Manual) and to act in accordance with the requirements of the ISMS. The consequences of security policy violations are described in the Forth Communication disciplinary policy. All staff will receive information security awareness training and more specialized staff will receive appropriately specialized information security training.

Availability

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network identified as part of the scoping work for section 1 of the Manual must be resilient and Forth Communication must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans.

Confidentiality

This involves ensuring that information is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to Forth Communication’s information and proprietary knowledge and its systems including its network(s), website(s) and data communications systems.

Integrity

This involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency for network(s), web site(s), and data back-up plans, and security incident reporting. Forth Communication must comply with all relevant data-related legislation in those jurisdictions within which it operates.

Physical (assets)

The physical assets of Forth Communication including but not limited to computer hardware, data cabling, telephone systems, filing systems and physical data files.

INFORMATION SECURITY POLICY

Information assets

The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, web sites, PCs, laptops and mobile phones as well as on CD ROMs, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means. In this context "data" also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc).

The ISMS is the Information Security Management System, of which this policy, the information security manual ("the Manual") and other supporting and related documentation are a part, and which has been designed in accordance with the specification contained in ISO 27001:2005.

A **SECURITY BREACH** is any incident or activity that causes or may cause a break down in the availability, confidentiality or integrity of the physical or electronic information assets of the company.

INFORMATION SECURITY POLICY

The Managing Director is the Owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements in clause A.5.1.2 in the Manual.
A current version of this document is available to all members of staff on *S:\Public\5. Security Policy* and within our hard copy document library. It does not contain confidential information and can be released to relevant external parties.

This information security policy was approved by the Board on **2 September 2005** and is issued on a version controlled basis under the signature of the Managing Director.

The ISMS security policy is in accordance with the Statement of Applicability, Version 2.3

This ISMS security policy has been approved by Forth Communication NI Ltd management and shall be reviewed by the management review team annually.

Signature:



Date: 17/04/08

Company Name	Forth Communication NI Ltd
Document Title	Security Policy
Author	Brian Nelson

Version No.	Status	Approved By	Issue Date
1.0	Initial issue	Brian Nelson	2 September 2005
1.1	Revision	Brian Nelson	17 April 2008
1.2	Revision	Brian Nelson	02 March 2010
1.3	Update due to SOA	Brian Nelson	15/11/2010
1.4	Update due to SOA	Brian Nelson	18/04/2011