

# UNIT4 Information Security Management Policy

**"To promote information security best practices and encourage vigilance over possible threats from any source under the guidelines of ISO 27001 as Information Security is the Foundation of our Business"**

## UNIT4's Commitment and Policy

UNIT4 is a company which is committed to preserving the security of its information assets. We have identified the information assets of the company, its customers and business partners which we need to proactively take action to protect. We promote information security best practices and encourage vigilance over possible threats from any source. To help us achieve our aim, we have created an information security management system which satisfies the requirements of BS EN ISO 27001 and have sought assessment and formal registration to the Standard.

- We have agreed our Information Security Objectives.
- We have a clear Information Security Policy.
- We insist that we are security-focused throughout the organisation.
- We have identified and evaluated our Information Security risks.
- We comply with relevant Legal and Regulatory requirements.
- We have defined everyone's Roles, Responsibilities & Authorities.
- We have appointed a Standards Compliance Director and Standards Compliance Manager.
- We recognise that effective Internal & External Communications are paramount.

Because..... **"Information Security is the Foundation of our Business"**

## Scope of the Information Security Management System

The Scope of our Information Security Management System is defined as -

*"The Design, Development, Sales, Marketing, Client Management, Customer Support, Training, Installation, ICT and Core Functions of UNIT4"*

## Our Information Security Policy

**It is our Policy to ensure that:**

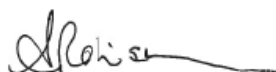
- Information will be protected against unauthorised access and disclosure.
- Confidentiality of information will be maintained.
- Integrity of information is protected from unauthorised modification.
- Regulatory and legislative requirements will be met .
- Business continuity plans will be maintained and tested (as far as practicable).
- All suspected breaches of information security will be reported and investigated,
- We ensure adequate prevention and detection of viruses and other malicious software,
- That appropriate training will be provided for all employees.

**We are also committed to:**

- assuring customers of full confidentiality.
- Identifying, through appropriate risk assessment, the value of information assets and to understanding the vulnerabilities and threats that may expose them to risk.
- Managing such risks appropriately.
- Complying with contractual requirements, procedures & practices and ISO27001:2005.
- Complying with applicable Legislation, as referenced in our Legal Register.

**We will set, monitor, achieve and review measurable objectives for the maintenance and improvement of our Information Security Management System. The ultimate forum for this will be the Management Review.**

Approved by Managing Director :



Date 08/03/2010

UNIT4 communicates this policy and the obligations/responsibilities required by the Information Security Management system to all its employees on their induction into the organisation. It has displayed its Policy on internal notice boards and has developed an area on its intranet dedicated to its Information Security Management System.

The responsibility of the upkeep of the Information Security Management system lies with:

**Standards Compliance Director** – Angie Marlow - Ultimate responsibility for strategic direction, objectives and goals.

**Standards Compliance Manager** – Joanne Higginson - Responsibility for ensuring the requirements of the standard are implemented and maintained.

To re-enforce our commitment we have nominated Information Champions across our organisation. These individuals continually assess the activities within their teams to identify improvement and wherever possible to reduce any possible threat to security of data.

#### Information Security Champions

Education Student Development	Steve Thomas	Testing Dept	David Maher
Sales	David Bales	Education Customer Services	Gareth Harper
Administration/ Finance	Sara Merrells	Professional Services	Andrew Price
Technical Consultancy Services	Michael Wozzley	ICT	Jonathan Howes
UNIT4 CRM Development	Neil Beynon	ABW UK Development	Kirsty Gibbs
ABW Customer Support	Mike Westrupp	QL Personnel Development	David Habberfield
Marketing	Charlotte Cresswell	Finance	Sue Tozer
Personnel	Aimee Pinnock	SGH Administration	Kimberley Seymour
Client Management	Sara Douglas	Education Finance Development	Raymond Mitchell

#### Staff Responsibility

All staff are responsible for considering how their actions can effect information security and they are encouraged to take an active role in the environmental management system. In practice this means all staff:

- Ensuring that any sensitive information that they are required to handle is treated appropriately.
- In line with internal Policies, all confidential or sensitive information should be locked away in the appropriate project folder when it is not in use, particularly outside office hours.
- Ensuring that, where practical, sensitive electronic documents are password protected.
- When it is necessary to send confidential or sensitive information to a customer, supplier or other third party, that this is completed in a secure manner.
- If emailing electronic files, ensure those files are password protected with the password being passed on to the recipient separately.
- If files are to be copied to a CD/DVD, ensure they should be password protected with the password being passed on to the recipient separately.
- If sensitive information is being delivered by post, the package should be marked "Private and Confidential" and a signature should be required upon receipt.
- Ensure once information is no longer required it is disposed of in a secure manner.
- If it is necessary to archive sensitive information ensure it is clearly labelled as confidential and appropriately archived.

## UNIT4 Information Security Management Objectives & Targets

In order for us as a company and our staff to identify and monitor if we are successfully meeting our Information Security Management Policy, we have set Information Security Objectives and Targets across our organisation. This allows our performance to be regularly monitored and measured for success. Our Information Security and Targets are shown below:

#### General

- To ensure UNIT4 Services are operated securely and professionally through the Information Security Management System & Achieve ISO 27001 Certification by the end of qtr 1 2010
- To establish, evaluate & maintain an "Asset Register" & Statement of Applicability by November 2009
- To ensure optimum technical security is in place by the end of 2009 and to ensure ongoing review

## ISO 9001 (Quality Management) and ISO 27001 (Information Security Management)

Our Information Security Management System has been designed to fully integrate with our Quality Management System based on the requirements of ISO 9001 : 2000. As such all our procedures for Information Security Management are held within our Quality Management System all of which are stored centrally under:

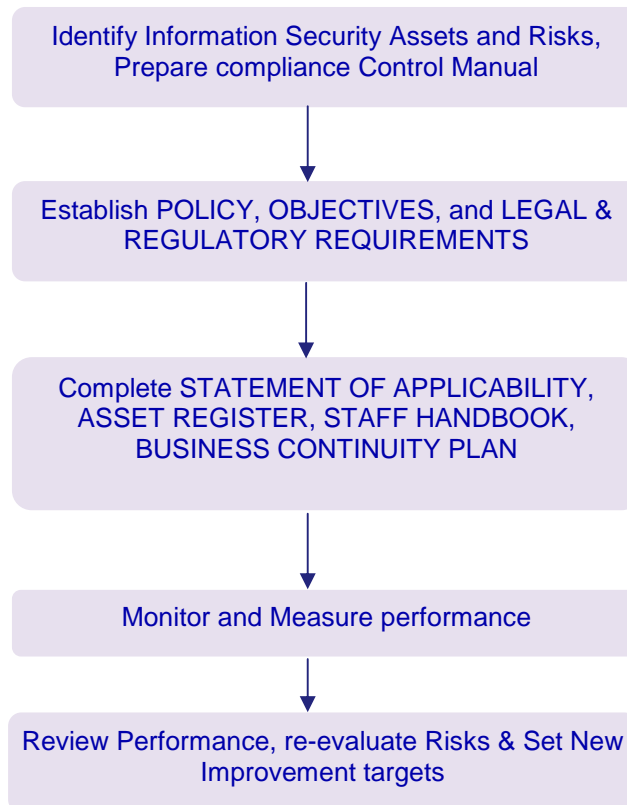
<http://44mossagruk/quality/Business%20Procedures/Forms/AllItems.aspx>

In addition we have created an area on our intranet site which is dedicated to Information Security Management System:

<http://44mossagruk/quality/IS/default.aspx>

This area is available to all staff and holds all our Information Security records and information.

Below identifies the steps taken to introduce and control the Information Security Management System.



Aspect	Impact	Legislation	Confirm Current Status	Obligation
Handling Investigations	Breach and risk of litigation	Regulation of Investigatory Powers Act 2000 (RIPA)	Checked via the Internet and other sources by JH	Compliance
Breach of Copyright	Loss of Licence	The Copyright Designs & Patents Act 1988	Checked via the Internet and other sources by JH	Stay Legal
Information Security	Loss of Reputation	The Human Rights Act 1998	Checked via the Internet and other sources by JH	Compliance
Information Security	Theft of Data. Competitive attack	Data Protection Act 1998	Checked via the Internet and other sources by JH	Safeguard data
Illegal Trading	Business Closure	Companies Act 2006	Checked via the Internet and other sources by JH	Stay Legal
Breach	Fines, Prison, Reputation	Computer Misuse Act 1990	Checked via the Internet and other sources by JH	Stay Legal
Breach	Litigation	Freedom of Information Act 2000	Checked via the Internet and other sources by JH	Stay Legal
Breach	Litigation	Telecommunication (Lawful Business Practice) (Interception of Communications) Regulations 2000	Checked via the Internet and other sources by JH	Stay Legal

