Unit4 Information Security Management Policy

"To promote information security best practice and encourage vigilance over possible threats 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, our 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 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 recognise that effective Internal & External Communications are paramount.

Scope of the Information Security Management System

"The Design, Development, Provision and Support of Unit4 Software Products and Associated Consultancy, Technical and Managed IT Services. Statement of Applicability v5."

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.
- Availability of information is upheld when required.
- We comply with applicable legislation, contractual requirements, procedures & practices and ISO27001.
- 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.
- 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 – and managing such risks appropriately.

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 UK&I:  **Date: April 2019**

Information Security Responsibilities

Unit4 communicates this policy and the obligations / responsibilities required by the Information Security Management System (ISMS) to all our employees on their induction into the organisation. We have displayed this Policy on internal noticeboards and have developed an area on our intranet dedicated to our ISMS. The responsibility of the upkeep of the Information Security Management system lies with:

Finance Director – **Matt Overd** – Ultimate responsibility for strategic direction, objectives and goals.

Facilities & Compliance Manager – **Donna Traves** – Responsibility for ensuring the requirements of the standard are implemented, maintained and has responsibility for reporting on its performance. Supported by the Standards Compliance Team.

Staff Responsibility

All staff are responsible for considering how their actions can affect information security and they are encouraged to take an active role in the information security 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 mobile device, ensure they are 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.

How do we achieve this?

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 objectives are set by our Finance Director and reviewed at least annually

Procedures and Records

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

Our ISMS has been designed to fully integrate with our Quality Management System (QMS) based on the requirements of ISO 9001. As such all our ISMS procedures are held within our Quality Management System all of which are stored centrally. This area is available to all staff and holds all our Information Security records and information.

Information Security Operational Control

Below are the key steps taken to introduce and control the ISMS.

- Identify Information Security Assets and Risks and prepare compliance control manual
- Establish POLICY, OBJECTIVES and LEGAL & REGULATORY requirements
- Complete STATEMENT OF APPLICABILITY, ASSET REGISTER, STAFF HANDBOOK and BUSINESS CONTINUITY PLAN
- Monitor and Measure PERFORMANCE
- Review Performance, re-evaluate risks and set new improvement targets

Unit4 has considered the security requirements of our stakeholders and has implemented security controls to meet the expectations of the market.

Legal Register

Compliance with Legislation

To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements Unit4 carry out a review of compliance with legislation annually.

We have defined all relevant statutory, regulatory and contractual requirements and our approach to meeting these requirements within our Register of Information Security Legislation

We ensure compliance on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

Records are protected from loss, destruction and falsification and data protection and privacy is ensured and supported by the Unit4 Data Protection Policy.

Managers ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards which in turn helps us to comply with legislative requirements.

Changes in legislation requirements will be reflected in the Register of Information Security Legislation.