In Business for You

Information Security Policy

September 11, 2024
Version 1.01

Public

Contents

1. Introduction

Unit4 is a company committed to preserving the confidentiality, integrity, and availability of physical and electronic information assets throughout the organization. Unit4 promotes information security best practices and encourage vigilance over possible threats from any source.

To achieve Unit4's goals and strategic objectives, an information security management system (ISMS) has been implemented.

Unit4 has achieved global certification to ISO 27001 and ISO 9001, and achieved ISO 27017 for relevant Cloud Operations. Unit4 publishes SOC1 and SOC2 reports for SaaS services delivered from the Microsoft Azure and Nordic Data Center. To ensure the ISMS controls and procedures are adhered to, Unit4 will undergo annual external audits of the scoped controls and formal registration to the Standards.

Unit4 maintain Information Security objectives.

- Unit4 global security policies are reviewed and approved annually.
- Information Security risks are identified and evaluated.
- Relevant legal and regulatory requirements are complied with.
- Unit4 has defined roles, responsibilities, and accountabilities.
- Unit4 understands effective internal & external communications are paramount.

2. Purpose

This policy defines requirements for information security to protect against the loss of confidentiality, integrity, and availability.

3. Scope

This policy applies to all users with access to Unit4 systems and equipment, information and data (these terms may be used interchangeably). This includes employees, contractors, temporary workers, or any other users.

Within the scope of the ISO 27001:2022 and ISO 27017:2015 certification:

> "The Design, Development, Provision, Support and Operations of Unit4 Products and Associated Services – Statement of Applicability v1.0"

4. Responsibilities

All users are responsible for information security and compliance as defined in this policy.

The responsibility for the Information Security Management System lies with:

- Unit4 Board of Directors: Responsible for overseeing Unit4 - https://www.unit4.com/about-us/board-of-directors/.

  - Audit and Risk Committee: Subset of the Board of Directors, responsible for monitoring the overall risk management, audit process and internal controls.
- Global Leadership Team (GLT): Responsible for guiding Unit4 teams - https://www.unit4.com/about-us/leadership-team.
- Chief Information Security Officer – Responsibility for strategic direction, objectives, and goals. Reports to subcommittee of GLT on security performance and risk.
- Compliance Managers – Responsibility for ensuring the requirements of the ISMS are implemented, maintained and have responsibility for reporting on performance.
- Security Champions: Embedded across the organisation, as required.

Unit4 communicates this policy and the responsibilities required by the ISMS to employees and display this Policy on the dedicated Unit4 Sharepoint site.

4.1. All users

All users are responsible for considering how their actions can affect information security and are encouraged to take an active role in the information security management system, in line with internal policies and procedures by:

- Handling information with care.
- Protecting passwords and devices.
- Communicating with caution.
- Taking care when using internet, email, and social media.
- Keeping premises secure.
- Reporting security incidents and data breaches.
- Keeping up to date with training.

4.2. Cloud Operations Team

Cloud Operations is led by Senior Director of Cloud Operations with the following responsibilities:

- End to end delivery of Cloud services based on IaaS and PaaS solutions, across regions, technology stacks as well as through all stages of customers' journey (migration / onboarding, BAU, contract termination and exit).
- Cooperation with all relevant internal and external stakeholders to provide uninterrupted, secure, and scalable value stream.
- Delivering innovation together with Development & Architecture teams while overseeing continuous cost monitoring and control to promote alignment of cloud usage and business value within the Financial Operations framework, in addition to ensuring that all services are following all security best practices.

5. Policy

- Protect information against unauthorised access and disclosure.
- Maintain confidentiality of information.
- Protect integrity of information from unauthorised modification.
- Uphold availability of information when required.
- The ISMS is subject to continuous, systematic review and improvement.

- Unit4 complies with applicable legislation, contractual requirements, procedures, and compliance with all Standards in scope.
- All suspected breaches of information security and data will be reported and investigated.
- Unit4 is active in the prevention and detection of viruses and other malicious software.
- Appropriate training is provided for all users.
- Risk Management Policy is in place, identifying and assessing risk to understand the vulnerabilities and threats to Unit4.

5.1.1. Objectives and Targets

To monitor and review if Unit4 are successfully meeting the Information Security Policy, objectives and targets have been set. This allows Unit4's security performance to be regularly monitored and measured for success.

5.1.2. Procedures and Records

ISMS policies, procedures and guidelines are held within the Unit4 intranet and holds all relevant documentation and information.

5.1.3. Operational Control

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

- Identify relevant risks.
- Established policy, objectives and legal & regulatory requirements.
- Completed Statement of Applicability, policies, procedures and incident response plan.
- Monitor and measure performance.
- Review performance, re-evaluate risks and set new targets.

Unit4 has considered the security requirements of stakeholders and interested parties and has implemented security controls to meet the expectations.

5.1.4. Legal Register

- To avoid breaches of law, statutory, regulatory or contractual obligations, and of security requirements, Unit4 maintain a Legal Register.
- Changes in legislation requirements are reflected in the Legal Register.
- Unit4 comply with 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, 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, complying with legislative requirements.

5.1.5. Global Cloud Operations

Unit4 Global Cloud Operations is a business unit of Unit4, which is responsible for deploying and maintaining Unit4 applications running in the cloud. Applications are delivered in a Software as a Service (SaaS) cloud service model. Cloud Operations supports many customers, partners, and government organizations that span across various services, geographies, and industries.

6. Exemptions

This policy should always be followed in the first instance, however if there are business cases where a user cannot reasonably conform with this policy, the Exemption Request Procedure must be followed.

7. Violations

Any suspected policy violations should be reported to security@unit4.com.

An employee found to have violated this policy may be subject to disciplinary action, including termination and potential civil and criminal liability. The use of the company's information systems and information assets is a privilege that may be limited or revoked at any time.

8. Version Control

Version	Date	Author	Summary of changes and Approval
1.0	December 07, 2023	Kirsty Dalby Claus Larsen	Updated to reflect global alignment of ISMS. Version changed to 1.0 due to policy framework update. Approved by GLT.
1.01	September 11, 2024	Kirsty Dalby	Minor updates to responsibilities and inclusion of Cloud. Update to 2022 revision of the ISO 27001 standard. Approved by CISO in Management Review.