In Business for You

Global Information Security Program Overview

August 20, 2024

Version 1.01

Public

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. This document should be reviewed in conjunction with Unit4 Information Security Policy (see Terms & Conditions | Unit4).

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 global security policies are reviewed and approved annually.
- Unit4 maintain Information Security objectives.
- 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.

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.

2. Information Security Organization

Unit4 has a dedicated Information Security team to ensure the security and integrity of systems and data. Security is embedded throughout the organization through training of security best practices.

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.

2.1. 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.

3. Risk Management

Unit4 has implemented a process for identifying, measuring, managing, report on, and addressing security related risks. This is used globally throughout the company and are regularly reviewed, reported on to leadership for visibility and prioritization of remediation activities.

4. Incident Management

Security incidents or suspected incidents must immediately be reported to ensure a quick and effective response. Incidents will be assessed by the incident response team to classify, determine urgency and scope. Incident response, containment, resolution, and post incident analysis will take place as required. Customers will be communicated with as necessary.

5. Compliance

5.1. Internal Audits

Internal audits are carried out frequently across the organisation to identify vulnerabilities and ensure the security policies are being complied with. Results will be reported to management and findings followed up on.

5.2. Compliance

Unit4 maintains strong business operations founded on high industry standards and adhering to the latest compliance and regulatory requirements. The compliance framework gives customers confidence that high levels of security and data protection practices will be met.

- SOC 1: Report for service organisations which are relevant to the user entities' internal control over financial reporting.
- SOC 2: Report for service organization with controls for Trust Services Principles, which are security, availability, processing integrity, confidentiality and privacy.

- ISO 27001: Provides requirements for establishing, implementing, maintaining and continuously improving the ISMS.
- ISO 27017: An information security management system guideline dedicated to Cloud computing.
- ISO 9001: This standard provides requirements for continuous improvement and quality management.

Unit4 has different service offerings, please check the service description to verify which standards apply.

6. Data Centres

Cloud Operations rely on data centres that feature state of the art facilities. These facilities ensure the highest level of security for customer data and platform infrastructure.

6.1. Asset Management

Data centre has implemented a formal policy that requires assets used to provide the services to be accounted for, updated and have an asset owner.

6.2. Controlled Access Points

Data centres are located in non-descript buildings that are physically constructed, managed, and monitored 24-hours a day to protect data and services from unauthorized access as well as environmental threats. Data centres are surrounded by a fence with access restricted through badge-controlled gates.

Pre-approved deliveries are received in a secure loading bay and are monitored by authorized personnel. Loading bays are physically isolated from information processing facilities.

CCTV is used to monitor physical access to data centres and the information systems. Cameras are positioned to monitor perimeter doors, facility entrances and exits, interior aisles, caged areas, high-security areas, shipping and receiving, facility external areas such as parking lots and other areas of the facilities.

6.3. User access

Access to buildings is controlled, and access is restricted to those with card reader (swiping the card reader with an authorized ID card) or biometrics for entry into data centres. Front desk personnel are required to positively identify employees or authorized contractors without ID cards. Staff must wear identity badges at all times and are required to challenge or report individuals without badges. Guests must be escorted by authorized data centre personnel.

6.4. Unauthorized Persons Entry

Employees and contractors must have a business need to enter a data centre and have received prior approval. Doors between areas of differing security require authorized badge access, are monitored through logs and cameras, and audited on a regular basis.

6.5. Secure Area Authorization

Data centre entrances are guarded 24x7x365 by security personnel and access is controlled through security personnel, authorized badges, locked doors and CCTV monitoring.

7. Network, database & application security

7.1. Network Level Security Features, Process and Protocols

- Secure access points and transmission protection: All traffic is secured using industry standard protocols such as SSL/TLS and HTTPS. The latest setup can be verified at www.ssllabs.com, using the product base URL applicable, such as erpx.unit4cloud.com, ubw.unit4cloud.com or u4f.unit4cloud.com.
- System security: Logical authentication and authorization mechanism in place.
- Firewalls: Stateful firewall technology to ensure only legitimate data enters the service environment.

7.2. Database Level Security Features, Process and Protocols

- Data security: Logical authentication and authorization mechanism in place.
- Databases and backups are encrypted using whole database encryption technology such as Transparent Database Encryption (included in Shared, option in Dedicated).

7.3. Application Level Security Features, Process and Protocols:

- Application access only: Unit4 software architecture consists of separate and distinct user interface (screen), business logic and database tiers. This separation means that access to the user interface tier is distinct and does not provide direct access to the underlying business logic and database tiers.
- User/Role level permissions: Unit4 applications allow for advanced granular permissions (Read, Write, Update, Delete) defined either by user or role and fully managed by the customer without Unit4 involvement.
- Data level permissions: Within a defined set of user/role permissions, Unit4 applications allow for granular filtering of data, such as restrictions of which customers a user is able to view or post invoices against.
- Idle disconnect: Sessions are automatically logged out after a certain period of inactivity in order to protect accounts if users inadvertently forget to log out.

8. Antivirus and malware protection

Malicious software is a serious threat and can have far-reaching consequences for the continuity of Unit4 SaaS. Unit4 uses the latest version of industry standard solutions to provide virus and anti-malware protection. Frequent application of security patches and updates helps protect systems from known vulnerabilities. Intrusion and malware detection systems are designed to detect and mitigate risks from outside attacks.

9. Security testing

Periodic vulnerability and security tests take place to validate Unit4 SaaS. Both vulnerability and security tests are performed by an independent third party. Penetration tests include:

- Authentication
- Authorization
- Session management
- Info disclosure
- SQL Injections and input validation
- Encryption

Unit4 releases on request and under NDA, the summary report made by the external penetration tester containing all vulnerabilities found, but excluding details of how to exploit the vulnerability.

Unit4 conducts monthly vulnerability scans of the servers managed by Unit4 using automated tools. Identified vulnerabilities are tracked until resolved, with reports available for Cloud Operations management.

10. Data Centre Operations

All information on data centres regarding cloud operations and reliability, security, privacy and compliance can be found on the respective websites.

10.1. Microsoft Azure

Details of Microsoft Azure can been found in the Microsoft Trust Centre:
https://www.microsoft.com/en-us/trustcenter/security/azure-security

10.2. Amazon Web Services

Details on AWS data centre security:

https://aws.amazon.com/security

10.3. Operating on Other Data Centres:

In case additional assurance is required for other data centre operations, please contact Unit4.

11. Information Disposal

Data stored on media including hard drives and tapes are destroyed in a safe manner. Unit4 follows current industry standards on media sanitization, which address the principal concern of ensuring that data is not unintentionally released. These guidelines encompass both electronic and physical sanitization. Data centre providers follow secure disposal processes which are verified as part of their compliance activities.