# Security Program

# For Unit4 Global SaaS Operations

# Security Program for Unit4 Global SaaS Operations

## Introduction, overview and objective

Unit4 Global SaaS Ops, the global unit responsible for Global solutions deployed in the Public and Dedicated Cloud, is designed and managed with the highest level of security and integrity in mind. Unit4 already holds different compliancy standards all over the world, where Unit4 Global SaaS Ops, as a new unit and running on a new platform (Microsoft Azure), is in the progress of adopting to all compliance standards. This process should be finished by the end of 2017.

Unit4 Global SaaS Ops uses the following definition of information security - the total of standards, plans and measures to guarantee the availability, confidentiality and integrity of the information systems provisioned and operated by Unit4 Global SaaS Ops.

The general objective of the Unit4 Global SaaS Ops Security Program is the establishment, recording and communication of objectives, key points and preconditions with regard to the security of the information systems provisioned and operated.

**Quality aspects** – consisting of confidentiality, integrity and availability, used to guide policies related to information security.

**Availability –** assuring that information is available to authorized parties when the information is needed, ensuring:

- continuity
- timeliness

**Integrity –** assuring the integrity of the information provision comprises of measures that, with regard to data, software and information distribution, ensuring:

- accuracy and consistency
- validity
- completeness
- verifiability
- authenticity

**Confidentiality** - assuring the confidentiality of the information provision comprises of measures that ensure the exclusivity of information: programs, data and equipment are only accessible for those who have explicitly been authorized.

## Compliance

The Unit4 Global SaaS Compliance Program gives Customers confidence that the highest levels of security and data protection practices will be met and allows Customers to streamline their own compliance with regulatory and industry standards.

- **SOC 1 Type 1** – Report for Service Organization with SSAE16 guidance which are relevant to 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 an Information Security Management System (ISMS).

- **PCI DSS** – Provides a baseline of technical and operational requirements designed to protect payment cardholder data. PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data.

*** Note: Third party compliance audits will be performed against the Unit4 Public and Dedicated Cloud environments operating on Microsoft Azure during 2017.**

Should government regulatory bodies specify requirements for certifications regarding HIPAA, FERPA, or other matters, Unit4 will make copies of such certifications available to Customer where such certifications are held by Unit4, or arrange for copies from Unit4's infrastructure provider as required.

Unit4 Global SaaS Ops uses Microsoft Azure, which holds a broad range of compliance certifications specified per industry and/or region.


## Physical Security

Unit4 Global SaaS Operations rely on Microsoft Azure that feature state of the art facilities. These facilities include, at minimum, the following characteristics to ensure the highest level of security for customer data and platform infrastructure.

Data center Security - Asset Management

Microsoft Azure has implemented a formal policy that requires assets (the definition of asset includes data and hardware) used to provide Microsoft Azure services to be accounted for and have a designated asset owner. Azure asset owners are responsible for maintaining up-to-date information regarding their assets.

Data center Security - Controlled Access Points

Microsoft data centers receive SSAE16/ISAE 3402 Attestation and are ISO 27001 Certified. Microsoft data centers 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 centers 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 centers 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.

Data center Security - Equipment Identification

MCIO, and consequently Azure, maintains a current, documented and audited inventory of equipment and network components for which it is responsible. MCIO employs automated mechanisms to detect discrepancies in device configuration by comparing them against the defined policies. MCIO turns off unused ports by default to prevent unauthorized access.

Microsoft Azure Fabric Controlled Hardware Device Authentication maintains a set of credentials (keys and/or passwords) used to authenticate itself to various Microsoft Azure hardware devices under its control. The system used for transporting, persisting, and using these credentials is designed to make it unnecessary for Microsoft Azure developers, administrators, and backup services/personnel to be exposed to secret information.

Data center Security - User Access
Access to Microsoft buildings is controlled, and access is restricted to those with card reader (swiping the card reader with an authorized ID badge) or biometrics for entry into data centers. Front desk personnel are required to positively identify Full-Time Employees (FTEs) 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 Microsoft personnel.

Data center Security - Unauthorized Persons Entry
Azure employees and contractors must have a business need to enter a Microsoft data center 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. Failure to abide by the Microsoft Data center security policies means instant dismissal for the employee.

Data center Security - Secure Area Authorization
Data center entrances are guarded 24x7x365 by security personnel and access is controlled through security personnel, authorized badges, locked doors and CCTV monitoring.

## Network, Database and Application Security

### 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.
- System security – Logical authentication and authorization mechanism in place.
- Firewalls – Stateful firewall technology to ensure only legitimate data enters the service environment.

### Database level security features, process and protocols

- Data security – Logical authentication and authorization mechanism in place.
- Database security – Every customer has their own secure database which means partitioning of databases is not required and customer data is not co-mingled. The outcome is that a customer's data is never inadvertently shared with others.
- Databases and backups are encrypted using whole database encryption technology such as Transparent Database Encryption.

### 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.

## Antivirus and Malware Protection

Malicious software (malware, viruses, ransom ware, etc.) is a serious threat for IT infrastructures. The impact of malicious software can have far-reaching consequences for the continuity of Cloud services. This plan describes the actions that are taken in the event that malicious software is detected in the Cloud service. All systems have antivirus software installed and are monitored to ensure the software is up to date as part of daily recurring preventive maintenance tasks.

**Preventive measures:**

1) Double-check that all antivirus software is up-to-date.
2) Check whether supplier provides separate preventive tooling.
3) Start preventive scan for other Customers.

**Active measures**

1) Determine the source of the virus.
2) Repair damage:
    a. Business critical aspects first.
    b. Isolate contaminated systems or connections (switch off everything that is suspect).
    c. Clean systems using software or tools.
    d. If restore: place in quarantine location first in order to establish whether there is any contamination in the backup.
3) Update problem analysis with actions taken.

## Response and Notification Plan

Response and customer notification (where applicable) is handled as part of overall our information security process.

**Response and Notification Plan: Data Breach**

In the event of a breach, affected Customers will be notified of impact of a breach within 2 to 4 hours followed by a response plan as determined by the nature, circumstances and severity of the data breach incident.

**Response Plan: Antivirus and Malware Protection**

Based on scan results, vulnerabilities are reported according to 5 levels of severity. Higher levels of severity trigger quicker response and resolution times. Specific timelines are dictated by nature of the incident and prescribed resolution. Action plan is as follows:

1) Symptoms of the virus.
2) Impact of the virus.
3) Method of spreading.

4) Determine impact/risk analysis for other Customers.
5) Reporting and communication.
6) Quantify damage for the Customer.

### Response Plan: Internal Operational Procedures

Security incidents are reported and recorded. In order to be able to react appropriately to security incidents that may occur, these incidents will be classified. After a security incident is resolved, an evaluation takes place, and possible measures will be taken to prevent comparable incidents in the future or to limit the consequences of an incident. Users who notice a (suspicion of an) incident or violation of the information security will report this to the Information Security Officer. He/She will take care of classifying the incident and of further settlement. Depending on the classification, the Information Security Officer will notify management and the Manager Global Cloud Operations.

## Audit and Security Testing

### Audits

Internal and external audits are conducted on a regular basis including engaging 3rd parties to perform penetration testing of our Cloud infrastructure.

### Security Testing

Periodic vulnerability and security tests take place to validate the Cloud solution. Both vulnerability and security tests are performed by a selected third party. Penetration tests include:

- Authentication
- Authorization
- Session management
- Info disclosure
- Injections and input validation
- Encryption
- 3rd party software.

Unit4 does not externally release audit reports and results of security tests. External, customer-facing summary reports are produced by third party auditors can be made available upon request and under NDA.

Unit4 conducts periodic (quarterly) testing of our internet facing systems. This includes a vulnerability test for the infrastructure and an application scan, including cross-scripting scan and other vulnerabilities identified by Open Web Application Security Project (OWASP), the National Vulnerability Database (NVD) or similar entities. Test results and other details are internal only.

## Operating on Microsoft Azure

All information on Microsoft data centers with regard to Cloud operations and reliability, security, privacy and compliance, can been found in the Microsoft Trust Center: https://azure.microsoft.com/en-us/support/trust-center/. Aspects of designing Cloud servers and sustainability can be found here: https://www.microsoft.com/en-us/server-cloud/cloud-os/global-datacenters.aspx.

For more information on core services controls regarding security, privacy, compliance and risk management please visit : https://cloudsecurityalliance.org/star-registrant/microsoft-azure/.

## Internal Operational Procedures

### Background checks for staff

Formal policies and procedures are established to delineate the minimum standards for logical access to platform and infrastructure hosts. Criminal background checks are conducted, as permitted by law, as part of pre-employment screening practices for employees, and commensurate with the employee's position and level of access. The policies also identify functional responsibilities for the administration of logical access and security.

### System access

Process and procedures have been established of who has access to data, which include system administration procedures such as identity management, access policies. Accounts are reviewed every 90 days; explicit re-approval is required or access to the resource is automatically revoked. Access is also automatically revoked when an employee's record is terminated. Requests for changes in access are captured in a permissions management tool audit log. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked.

### Information Disposal

Data stored on media including hard drives and tapes are destroyed in a safe manner if they are defective. Unit4 follows NIST 800-88 Guidelines on Media Sanitization, which address the principal concern of ensuring that data is not unintentionally released. These guidelines encompass both electronic and physical sanitization.