Security Measures
(Technical and Organisational)

Unit4 Business Security Measures (Internal business operations summary)

Description of the technical and organizational security measures implemented by the Processor in its organization. More details about the Security Policy and Security Program can be found at www.unit4.com/terms.

Physical Security, Unit4 premises:

- Physical access control is managed by Unit4 workplace experience.
- All offices have security systems in place in respect of controlling access, e.g. manned reception desks, access-controlled doors, alarmed fire doors, intruder detection systems and/or lockable offices.
- Unit4 operates access controls with the help of what people know, such as password or personal access code; and/or with the help of what people carry, such as a security pass.
- Communication rooms have additional physical controls.
- Access to secure areas or sensitive/confidential information is restricted to prevent unauthorized access by way of lockable offices or lockable cabinets and operating clear desk policies.
- Visitors are controlled at reception.
- Shredders or other suitable secure disposal methods for sensitive documents are used.

Virtual and computing Security:

- Line managers will ensure employees and contractors return all Unit4 assets in their possession upon termination of their employment or contract agreement. Records of return of assets are maintained.
- Unit4 classifies and protects information according to its classification of public, proprietary, confidential or sensitive.
- Media (including hard drives) are disposed of securely and safely when no longer required. All sensitive material (hard disks, floppies, etc.) is removed by guaranteed removal software, (not by reformatting or deletion) before disposal or physical destruction.
- Anti-malware is in place using the latest version of industry standard solutions to provide virus and anti-malware protection.
- Controls are in place for assigned rights.
- Logging and access control is utilized.
- Business Continuity and Disaster Recovery plans have been prepared which include information security considerations.
- Recovery measures are in place allowing for restoration of data in a timely manner in case of an incident.

Information Security Policies and Documentation:

- The Global Leadership Team for Unit4 and/or its respective local management teams have oversight of both global and local information management and security plans including any information security policies that meet identified information security risks and supports the business goals.
- Information security and management is assigned globally to the Chief Information Security Officer and Global Data Protection Officer, who manage resources to deliver strategic and overall compliance with information security policy and process.
- Unit4 has implemented security policies that are approved by top management, reviewed and updated regularly to comply with good industry practice.
- These policies address security risks and support business goals.
- Responsibility for the information security management system lies with the Chief Information Security Officer, with oversight from Unit4 top management as defined in the Information Security Policy.
- Unit4 provides all employees with training in relation to security; data protection; business principles and ethics.
- Unit4 has published on www.unit4.com/terms: Data Processing Policy; Privacy Statement; and other information relevant to privacy at Unit4 including a Data Handling FAQ.
- Unit4 has appointed a Global Data Protection Officer.
- Unit4 enters into non-disclosure and confidentiality agreements with Third Parties when sharing confidential information relation to its business.
- Unit4 ensures all employees and contractors enter into standard confidentiality clauses in their contracts.

Data privacy and security by design

- Unit4 SaaS applications are designed with data privacy and security in mind. Unit4 is continually improving the security of its solutions, by applying lessons learned from annual penetration tests and audits.
- Unit4 and the data center operators who provide infrastructure on which Unit4 SaaS is provided hold various security certifications, for details please refer to the applicable Service Description.

Data breach notification

- Unit4 shall notify the Customer within the timescales agreed with the Customer in the Agreement. Customer should make sure that the contacts listed in Unit4 Support Portal are always up to date, as they will be used for all communication.

Unit4 SaaS on Microsoft Azure (summary)

Technical and organizational security measures have been implemented by the Processor in relation to Unit4 SaaS on Azure.Unit4 utilizes several mechanisms to protect data in the cloud. Below is an overview of applied controls.

Network level security

- Secure data transmission over public networks – all traffic is secured using industry standard protocols such as SFTP, SSL/TLS and HTTPS.
- Logical authentication and authorization mechanisms in place.
- Next generation firewall technology to ensure inbound and outbound traffic is controlled.

Database level security

- Logical authentication and authorization mechanisms in place.
- Every customer has their own secure database ensuring that customer data is not co-mingled. See Data Segregation.
- Databases and database backups are encrypted using whole database encryption technology such as Transparent Database Encryption.
- Non-transactional data and files will be secured by standard symmetric encryption such as AES.
- Azure Key Vault is used to maintain control of keys used by cloud applications and services to encrypt data.

Vulnerability Management

- Cloud infrastructure, cloud services, products, devices and internal resources is closely monitored by a specialized team.
- Penetration testing of applications and infrastructure is carried out on a periodic basis.
- Vulnerability scanning is carried out periodically to detect and assess potential vulnerabilities in our applications and infrastructure.
- Unit4 is continuously monitoring and risk assessing the effectiveness of our vulnerability program to improve and secure our applications and infrastructure.

Disaster Recovery

- High availability infrastructure.
- Tested periodically.

Threat detection, mitigation and response

- Unit4 is diligent in threat detection and response with centralized monitoring systems that provide continuous visibility and timely alerts.
- Security patches and updates are routinely applied helping protect systems from known vulnerabilities.
- Intrusion and malware detection systems are utilized to detect and mitigate risks from outside attacks.
- In the event of malicious activity, our incident response team follows established procedures for incident management, communication and recovery.

Data segregation

Unit4 takes the responsibility of protecting customer data very seriously and uses both technical and organizational controls to do so.

- Customer databases are encrypted with customer unique encryption keys.
- Data from multiple customers may be stored on the same cloud resource, however Unit4 uses logical isolation to segregate each customer's data from that of others. Unit4 SaaS is designed to counter risks inherent in a multitenant environment. See Database level security.

Data encryption in transit

- Unit4 provides, as a standard, secure access to all its services by encrypting all data in transit traveling on public networks.
- Only secure protocols are used such as HTTPS over TLS and using secure cipher suites.

Access control

- Customers are fully empowered to conduct front-end access control to their application. This means that the responsibility for creating new accounts, account termination and review is with the customer.
- Unit4 will retain limited back-end access to customer data (by direct database connection). Access by Unit4 shall be strictly limited to activities necessary for installing, implementing, maintaining, repairing, troubleshooting or upgrading the solution. All access is logged and limited to a small group of Cloud Engineers, Professional Services and Support Consultants.
- Access logs are saved in the centralized monitoring solution for 365 days. In case of data breaches, Unit4 can provide the access logs on request.

Unit4 SaaS hosted on Nordic Cloud data center (summary)

Technical and organizational security measures have been implemented by the Processor in relation to Unit4 SaaS delivery hosted in our Nordic Cloud data center offering. Unit4 utilizes several mechanisms to protect hosted data. Below is an overview of applied controls.

Network level security

- Secure data transmission over public networks – all traffic is secured using industry standard protocols such as SFTP, SSL/TLS and HTTPS.
- Logical authentication and authorization mechanisms in place.
- Next generation firewall technology is in place to ensure inbound and outbound traffic is controlled.

Datacenter security

- The Nordic Cloud data center offering is a Tier 3 data center offering with Full N+1 redundancy.
- Security features to protect the data centers includes Perimeter fences; Camera Surveillance, Stringent access control (Biometric); Stringent visitor control procedures; Airlocked access points and 24/7 monitoring of the facilities by guards.

Vulnerability Management

- Cloud infrastructure, cloud services, products, devices and internal resources is closely monitored by a specialized team.
- Penetration testing of applications and infrastructure is carried out on a periodic basis.
- Vulnerability scanning is carried out periodically to detect and assess potential vulnerabilities in our applications and infrastructure.
- Unit4 is continuously monitoring, and risk assessing the effectiveness of our vulnerability program to improve and secure our applications and infrastructure.

Disaster Recovery

- Redundancy built into the infrastructure to eliminate possible single points of failure.
- Disaster Recovery capabilities are tested periodically.

Threat detection, mitigation and response

- Unit4 is diligent in threat detection and response with centralized monitoring systems that provide continuous visibility and timely alerts.
- Security patches and updates are routinely applied helping protect systems from known vulnerabilities.
- Intrusion and malware detection systems are utilized to detect and mitigate risks from outside attacks.
- In the event of malicious activity, our incident response team follows established procedures for incident management, communication and recovery.

Data segregation

Unit4 takes the responsibility of protecting customer data very seriously and uses both technical and organizational controls to do so.

- Data from multiple customers may be stored on the same resource, however Unit4 uses logical isolation to segregate each customer's data from that of others. Unit4 SaaS Nordics is designed to counter risks inherent in a multitenant environment.

Data encryption in transit and at rest

- Unit4 provides, as a standard, secure access to all its services by encrypting all data in transit traveling on public networks.
- Only secure protocols are used such as HTTPS over TLS and using secure cipher suites.
- Stored data is written to the disk encrypted with 256-bit Advanced Encryption Standard (AES).
- Encryption keys are managed by Unit4.

Access control

- Customers are fully empowered to conduct front-end access control to their application. This means that the responsibility for creating new accounts, account termination and review is with the customer.
- Unit4 will retain limited back-end access to customer data (by direct database connection). Access by Unit4 shall be strictly limited to activities necessary for installing, implementing, maintaining, repairing, troubleshooting or upgrading the solution. All access is logged and limited to a small group of Cloud Engineers, Professional Services and Support Consultants.
- Access logs are saved in the centralized monitoring solution for 365 days. In case of data breaches, Unit4 can provide the access logs on request.
- Physical access to our Nordics Data centers follows the principle of least privilege. The data centers are tier 3 and has strict access control in place, requiring keycard, pin and biometric verification before secure areas can be accessed.

Unit4 SaaS on Amazon Web Services (summary)

Technical and organizational security measures have been implemented by the Processor in relation to Unit4 SaaS on AWS.

Unit4 utilizes the Amazon Web Services Center for Internet Security (CIS) AWS Foundations Benchmark standard, which is a set of best practices that automatically detects when AWS accounts and deployed resources do not align with security best practices within the CIS security controls. Any anomalies are reported with follow up actions in place to ensure compliance. This covers the Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, and Incident Response Management.

Additional Elements for Unit4 Platform Services (summary)

Technical and organizational security measures have been implemented by the Processor in relation to Unit4 Platform Services (SaaS). Unit4 Platform Services utilizes several mechanisms to protect data in the cloud. Below is an overview of applied controls.

Network level security

- Secure data transmission over public networks – all traffic is secured using industry standard protocols such as SFTP, SSL/TLS and HTTPS.

Database level security

- All data stored in storage accounts are encrypted at rest.
- All storage accounts require secure transfer – all traffic is secured using industry standard protocols such as SSL/TLS and HTTPS.
- All data stored in Azure Cosmos DB is encrypted at rest and in transport.
- All Azure SQL Servers are enabled with Transparent Data Encryption (TDE).
- All Azure SQL Servers are running with Threat detection and auditing enabled.
- Azure Key Vault is used to secure sensitive information such as service principal credentials.

Messaging level security

- All data stored by Azure Service Bus instances are encrypted at rest.
- All traffic (in transit) on the Azure Service Bus is secured using industry standard protocols such as SSL.

Authentication

- All services follow the principle of least privilege and authentication towards services and their APIs are secured using industry standard mechanisms.
- OpenID Connect and the underlying oAuth 2.0 protocol is used to securely perform authentication of users and/or client services with trusted parties and validate identity and access using claims-based tokens.
- HMAC (Hash-based Message Authentication) is used as an alternative method to secure communication between services.