Unit4 Talent Management

Unit4 Cloud Service Description

VERSION 1.0

September 2021

CONTENT

1. Introduction

Unit4 Talent Management (Unit4 TM) is a talent management and enablement solution for performance management, employee engagement and e-learning. Our cloud platform enables our Customers to build a culture of feedback and growth, increase engagement and reduce churn. There are three fundamental modules of Unit4 TM, which are: "Learn", "Engage" and "Perform".

Unit4 TM is highly adaptable when business needs change and provides a low cost of ownership.

The purpose of this Unit4 TM Service Description is to describe and detail the make up of the Unit4 SaaS made available to the Customer.

Unit4 provides a complete technically-managed solution for Unit4 TM deployed in the public cloud. This end-to-end Service includes infrastructure, hardware, system software, monitoring, management and maintenance of the entire solution (including backups), disaster recovery and Service updates.

Unit4 offers cloud enterprise solutions as Unit4 SaaS - a Software as a Service delivery model deployed on Microsoft Azure. This model leverages Microsoft Azure's scale and experience of running highly secure and compliant cloud Services around the globe. Microsoft Azure's infrastructure is second to none in terms of physical and electronic security, and it adheres to industry standards such as ISO 27001, SOC 1 & 2, PCI DSS and many more.

Unit4 TM is available as a shared option, where computing resources are shared between Customers without any interference.

In summary, Unit4 provides the following:

- Access to Unit4 TM over secure internet connections (HTTPS). A variety of browsers and mobile platforms are supported;
- Comprehensive integration options available, including the use of Unit4 APIs/web services and file-based interfacing;
- Fully scalable solution, in a high availability environment with redundancy;
- Relevant security level;
- Continuous monitoring is in place, feeding alerts and continuous improvement;
- Updates, patches and hot fixes on infrastructure managed by Unit4;
- Application Releases, Updates and Hot Fixes;
- Production Environment and Non-Production Environments and disaster recovery in a physically separate secondary site;
- Service Level Agreement, with Service Credits based on Service Availability;
- Unit4 Community (aka Community4U) to engage with Unit4 directly, giving insight in the Service performance indicators and see the status of Services; and
- Formal policies in place for: information security, data processing, disaster recovery, business continuity and acceptable use.

2. Data centers & data residency

Unit4 SaaS use the Microsoft Azure infrastructure and platform Services to deliver the Unit4 SaaS. These Services are delivered from within different geopolitical zones, using a primary

and a secondary location in every zone to meet KPIs and disaster recovery needs. The location within each geopolitical zone is at the discretion of Unit4 and can change from time to time. The table below contains details of the geopolitical zones, along with the data center locations. For more information, see Azure region details: azure.microsoft.com/regions.

Geopolitical zone	Provider	Data location (Countries/City's/Regions)	Time zone
EU	Microsoft Azure	Dublin, Ireland and Amsterdam (DR), Netherlands	CET/CEST
United Kingdom	Microsoft Azure	London and Cardiff (DR)	GMT/BST
Canada	Microsoft Azure	Toronto and Quebec City (DR), Canada	EST/EDT
Asia Pacific	Microsoft Azure	Singapore and Hong Kong (DR)	SGT/HKT

Unless agreed otherwise in an Order Form the chosen deployment of the Customer will be as follows:

Customer residence	Geopolitical zone used
EU, Norway	EU – Azure
UK, Australia/New Zealand	UK – Azure
South Africa	EU - Azure
Canada, US	Canada - Azure
Asia Pacific	Asia Pacific - Azure

3. Service model

Unit4 TM is available in a shared Multi-Tenant deployment model. In summary, the characteristics of mentioned model are as set out in the table below:

Category	Component	Characteristics
SOLUTION	All patching, updates of the standard solution (technical)	Included and automatic
INFRASTRUCTURE	Environments included	1 Production + 2 Non-Production (Preview and Acceptance)[1]
	Non-transactional storage (e.g. documents)	250GB + 2GB per each purchased FTE[2]
	Transactional storage (e.g. database)	Unlimited
	Availability guarantee	Yes
	Response time guarantee	Yes
	Data center	Microsoft Azure
SERVICES	Releases will commence	Automatically
	Updates will commence	Automatically

[1] Three (3) environments set up is a new standard applicable to Customers that got their Agreements signed with effect from May 2020.Please be informed that by default Customer is provided with 1 Production and 1 Non-Production Environment. Second Non-Production Environment is included in the offering, but has to be requested by the Customer separately via Service Request.

[2] Additional Non-transactional Storage can be requested by the Customer and is going to be a subject of extra charge.

Category	Component	Characteristics
	On-going technical operations, performance management, maintenance of all infrastructure components, monitoring alert response and issue resolution	Yes
	Backup	Yes
	Disaster recovery	Yes
	Monitoring program of infrastructure and application	Yes
COMPLIANCE	Compliance certificates and assurance documents	ISO 27001 ISO 27017[3]

4. Environments

As standard, Customer receives three (3) environments[4], including:

- One Production Environment (PE) called alternatively “live” environment, being the environment that the Customer uses to run the day to day (live) operation; and
- Two Non-Production Environments (NPEs):

[3] Unit4 TM is compliant with mentioned standards to give 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. It is Customers responsibility to ensure their own compliance with all applicable standards and compliance obligations. For more details around Information Security please see the Unit4 Information Security Policy, which is available at www.unit4.com/terms.

[4] Three (3) environments set up is a new standard applicable to Customers that got their Agreements signed with effect from May 2020.Please be informed that by default Customer is provided with 1 Production and 1 Non-Production Environment. Second Non-Production Environment is included in the offering but has to be requested by the Customer separately via Service Request.

- Preview – a Customer's Preview environment always contains the latest Updates for the Unit4 Product in use by the Customer. Can also be used as “Test”/“Quality”/“UAT” environment.
- Acceptance – which can be used according to Customer needs as “Test” / ”Quality” / ”Development” / ”Pre-Production”.

Unit4 assigns to every Customer a unique Customer ID code and the domain, which are visible in various elements of the Service (including environments) and they are used for Customer identification. The MS Azure Customers ID code is a 3-character acronym (applicable to Customers that already have other cloud product entitlements at Unit4) or combination of fixed 3 characters (TMA) and 3 digits (if Unit4 TM is the only Unit4 product that Customer is entitled to). The domain is established based on Customer’s name. The Customer ID codes and the domains are created at Unit4 discretion during the early stage of the implementation and are not a subject to change.

4.1 Production Environments

Only the Production Environment (PE) is subject to the SLA.

4.2 Non-Production Environments characteristics

Although a Non-Production Environment (NPE) is not subject to the SLA, NPEs have some characteristics as described below.

Update of an NPE to a new Update

The Preview environment is updated as soon as an Update is available. Once an NPE has been updated to the latest Update, it is not possible to move back to the previous Update.

5. Reporting and monitoring

5.1 Reporting on Service Performance

Unit4 provides operational information regarding Unit4 SaaS on the Unit4 Community4U. That information includes:

- Service Availability (NOTE: currently https://status.intuo.io);
- Average Response Time; (NOTE: currently https://status.intuo.io);
- Scheduled maintenance (times, dates per region);
- Release information and deployment schedules;
- Incidents overview;
- Site recovery status (in the event of the disaster plan initiation).

5.2 Monitoring program

A continuous 24x7 monitoring and resolution program is in place to detect and resolve incidents to meet the Unit4 Service Availability and response time targets on Production Environment.

6. Releases and updates

Periodically, Unit4 introduces new features in the Unit4 TM Service including enhanced features and functionality across applications. Features and functionality will be made available as part of a Release. As part of regular maintenance Unit4 will apply Updates and Hot Fixes, as deemed necessary by Unit4 in order to maintain the existing features of Unit4 SaaS and to maintain KPIs and security.

Releases and Updates will be provided free of charge as part of the Service. However, it should be noted:

- Any Releases or Updates may result in additional Configuration and/or functional adjustments that are required to be made by either: (i) the Customer; (ii) Unit4; or (iii) approved Service partner consultants, which are not included in the Unit4 SaaS and will be a subject to additional charges.

6.1 Release deployment

Releases may take place approximately four times per year. The frequency of Releases may be increased or decreased at Unit4's discretion. A schedule of planned deployment of Releases to the Production Environment will be published on Unit4 Community4U. A Customer's Preview environment always contains the latest Release for the Unit4 SaaS solution in use by the Customer.

6.2 Update Deployment

Updates are applied as deemed necessary by Unit4 cloud operations in order to maintain the existing features of the Unit4 SaaS as well as maintaining KPIs and security.

6.3 Hot Fix Deployment

Hot Fixes are applied as deemed necessary by Unit4 cloud operations in order to maintain the existing features of the Unit4 SaaS as well as maintaining KPIs and security.

7. Planned and unplanned maintenance

7.1 Planned Maintenance

Planned Maintenance windows are dedicated to apply all the respective changes to the Service provided e.g. solution Updates, Releases and infrastructure changes. During Planned Maintenance the Production Service may be periodically unavailable. You can find more details on schedule presented in the table below:

	Planned Maintenance windows (PMW) ***Updates, Releases and Infrastructure***
EU and United Kingdom regions	12 per year, **Regular PMW:** From: Sat 5PM To: Sat 11PM UTC* or **Extended PMW**: From: Sat 5PM To: Sun 5AM UTC*

*Time of Planned Maintenance window is a subject of a change (+/- 1hr), which is related to winter and summer time adjustments.

Planned Maintenance windows are subject to change upon reasonable notice. The exact dates of Planned Maintenance windows are communicated on Unit4 Community4U. By default all Planned Maintenance windows are regular and take up to 6hrs, unless they are promoted to extended Planned Maintenance windows, these take up to 12hrs.

If actual downtime for scheduled or Planned Maintenance exceeds the time allotted for Planned Maintenance, it is considered part of the calculation for Service Outage. If actual downtime for scheduled or Planned Maintenance is less than time allotted for Planned Maintenance, that time is not applied as a credit to offset any Service Outage time for the month.

Planned Maintenance can also be carried out by Unit4 provided that the Customer has received at least 8 hours' notice. This will occur in unforeseen or exceptional circumstances only (similar to emergency / Unplanned Preventative Maintenance) to deal with a vital or critical issue and Unit4 will use its reasonable endeavours to do this outside Business Hours to cause minimal disruption to the Customer. In this case, because Unit4 provides Customer 8 hours' notice, this maintenance does not count as Service Outage. This is so that Unit4 is not encouraged to wait until the next Planned Maintenance window to deal with an urgent issue and avoid a Service Credit.

7.2 Unplanned Preventative Maintenance

Unit4 may carry out Unplanned Preventative Maintenance if there is an urgent requirement to secure the stability, or the security of Unit4 SaaS. This action may be taken at the discretion

of Unit4 for unforeseen and exceptional circumstances, which require immediate resolution that cannot wait until the next Planned Maintenance window. Unplanned Preventative Maintenance is counted as a Service Outage.

8. Customer permissions and responsibilities

8.1 Customer permissions

Customer has the right to:

1) Monitor PE availability and Service Response Time on an active basis using a third-party monitoring Service. Monitoring acts as a consumer of the Unit4 SaaS and is subject to any and all present and future Usage Restrictions of the Unit4 SaaS. Customer and Unit4 must agree, prior to monitoring, on monitoring details in order to ensure that the monitoring does not interfere with the Unit4 SaaS offering and that Unit4 SaaS security tooling does not block the monitoring Service.
2) Conduct an external security vulnerability scan on an annual basis. Details of the planned scan must be provided to Unit4 at least 30 days in advance of each scan using a Service Request.
3) Conduct a security penetration test on an annual basis. Details of the planned test must be provided to Unit4 at least 30 days in advance of each test, using a Service Request.

Any activities to prepare, coordinate or manage the above by Unit4 is subject to additional charges.

8.2 Customer Responsibilities

Release and Service Updates

The following list summarizes typical Release and/or Update tasks and indicates Services included as part of the Unit4 SaaS and tasks that are the responsibility of the Customer (or Unit4 Professional Services at an extra charge):

Task	Included	Customer Responsibility
Project Planning		
• Publishing general availability schedule of Releases on the Unit4 Community4U	✓	

Task	Included	Customer Responsibility
• Managing timelines, outline goals, roles and responsibilities		✓
• Business analysis and discovery		✓
• Creating test plans		✓
Release deployment in Preview environment		
• Update Preview environment with data	✓	
• User training on changes		✓
• Test: conducting basic Release testing		✓
• Training support to assist with testing		✓
• Functional and User acceptance testing as desired		✓
• Training, implementation and Configuration for new features		✓
• Uplift and testing of all Integrations		✓
• Reviewing test scripts and testing outcome for issues resolution		✓
• Go/No-go criteria's and agreement on Production Release deployment timing		✓
Release deployment in Production		
• Update existing application Configuration, being all activities undertaken to set up application provided by the Service which involve the use of standard menus and functionality. There may be rare cases where it is not technically possible to determine the correct business Configuration; in these rare cases any tasks that must be completed manually are the responsibility of the Customer.	✓	✓
• Update Production Environment with Release	✓	

Technical & functional responsibilities

Technical environment responsibilities:

- Supply, administration and maintenance of customer-side client devices and local printers;
- Customer-side networking infrastructure, including connectivity to the internet;
- Security of Customer-side network, devices and internet connectivity;
- Ensuring sufficient bandwidth, including internet bandwidth;
- End-to-end ownership of conducting penetration tests, any security checks, as well as Customer owned monitoring.

Functional environment responsibilities:

- Customer is fully responsible for the Configuration and administration of the functional aspects of the Service, including User and role administration.

8.3 Customer Obligations

Account Set-up

Customer is responsible for designating its Users, and for ensuring that all Users are adequately trained and understand Customer's remote access and use obligations and requirement to comply with Unit4's acceptable use policy (www.unit4.com/terms). Where applicable each individual User must establish an Account. Customer is responsible for managing its Accounts and disabling a User's Account when Unit4 SaaS access is no longer required, including immediately upon termination of such User's affiliation with Customer. Customer is responsible for its Users 'acts and omissions and for all activities occurring under its Users 'Accounts.

Account Administrator

Customer will designate one or more Account Administrator(s). The Account Administrator(s) responsibilities include, but are not limited to, coordinating with Unit4 regarding the Unit4 SaaS and managing Customer's Accounts. Customer warrants that its Account Administrator(s) will maintain authority to act on Customer's behalf concerning the Unit4 SaaS, and that Unit4 can rely on the Account Administrator(s) actions and instructions in connection therewith.

Account Security

Each User is responsible for keeping his or her Account credentials confidential. Users may not share Account credentials, and Customer may not recycle Account credentials when activating or disabling Accounts. Customer will notify Unit4 immediately upon discovering any known or suspected unauthorized access to, misuse of, or breach of security for the Unit4

SaaS or its Users' Accounts, and will provide all information and take all steps requested by Unit4.

9. Integrations

Integrations are permitted and can be written by Unit4, Unit4 partners or the Customer. Maintenance, support, implementation and update considerations for integrations are not included in the Service fee. The Customer has full responsibility for all aspects of integrations deployment and maintenance (e.g. code lift for release version compatibility, functional testing, configuration and error resolution). Unit4 has no responsibility to maintain integrations compatibility or fix any problems.

9.1 Unit4 APIs backward compatibility

Unit4 recommends using the most recent version of the Unit4 APIs in order to receive optimum performance and stability. Prior versions of Unit4 APIs are updated to support backward compatibility for all prior versions of Unit4s APIs that have not reached an end-of-life status. End-of-life announcements will be made not less than eighteen (18) months before the end-of-life of each Unit4 API.

9.2 Integrations

Integrations, defined as any solution capability that shares data with an external, are permitted according to the guidelines described below. Interface methods not explicitly stated below are not permitted. In general, no direct database access is permitted at all.

Standard Unit4 product integration options:

Integration Type	Available?
Unit4 TM and ERP synchronization for Employees - Employment – Competencies – Positions and Organizational Structure	Yes
Synchronization with Outlook	Yes
Publish on Slack	Yes
Publish on MS Teams	Yes
Unit4 TM API/web services integrations	Yes

10. Technical operations

10.1 Connectivity

Access to the Web Client is delivered over the public internet using an HTTPS connection (RSA 2048 bits - SHA256 with RSA and/or EC 256 bits SHA256 with ECDSA).

Internet bandwidth suggestions*

As the configuration and use of Unit4 TM is highly variable Unit4 can provide only high level bandwidth suggestions; Unit4 TM (Web Client) – an assumed concurrency factor of 5 gives an average bandwidth requirement per User of 20 - 50 Kbps with a max latency of 100ms.

* Response times will be dependent upon a variety of factors such as number of Users, type of web processing initiated, Customer side internet line capacity and infrastructure set-up such as use of proxies.

10.2 Solution access

The Unit4 TM solution can be accessed in the following manner:

- Unit4 TM Web Client, accessed via a supported web browser;
- Programmatic access to Unit4 TM API/web services; or
- Unit4 TM mobile applications via APIs/web services.

10.3 Authentication

By default, authentication for Unit4 TM (Web Client) is carried out using application-based username and password authentication. Management of Users and passwords within the Unit4 TM application is the responsibility of the Customer.

The Unit4 SaaS has capabilities for federated authentication to allow Customers' Users to use their organizational credentials (e.g. domain username and password) when logging in to an Unit4 application using a web browser (web access). With federated authentication, the Customer's authentication provider (e.g. ADFS, Azure Active Directory, etc.) performs authentication instead of an application-specific username and password that is validated by the Unit4 application.

In order to use federated authentication there is an optional Service called Unit4 Identity Services or Unit4 IDS. Unit4 IDS is a Multi-Tenant identity solution and architecture for the Unit4 ecosystem, that allows Users to have one single identity across multiple applications and provides a single sign-on experience. More details about Unit4 IDS can be found in Unit4 IDS Service Description at www.unit4.com/terms.

The Customer is responsible for configuration of their identity provider (IdP) and to provide specific information (required or requested) to Unit4 that allows for configuration of Unit4 IDS.

Unit4 TM Authentication	Basic (Unit4 TM specific username and passwords)	Federated Authentication (via Unit4 IDS to Customer's IdP)
U4TM Web Client	Yes	Yes
U4TM Mobile	Yes	Yes

Preparing for the use of IDS requires an effort on gathering technical information to connect IDS with the Customer's Identity Provider. The implementation of this Service may require the involvement of the Unit4 Professional Services.

10.4 Technical overview

Topic	Description
Email	
Domain	Unit4 provides basic e-mail functionality for sending messages to recipients with the following domains: *.intuo.io (EU geopolitical zone) and *.tm.unit4cloud.com (United Kingdom geopolitical zone)
Protocol	SMTP over TLS
Authentication	
Protocols supported	All the supported protocols can be found in Unit4 People Platform Service Description at www.unit4.com/terms.
Internet communication	
Protocols supported	HTTPS (browsers supporting TLS >1.2 are required) secured with RSA 2048 bit keys and SHA256withRSA encryption and/or EC SHA256 with ECDSA .

11. Data considerations

11.1 Transfers of Customer Data to the Unit4 TM

Unit4 deploys a standard architecture and therefore, where Customer is an existing Unit4 Customer, the Customer is responsible for ensuring data consistency (i.e. that Customer Data to be inserted follows such standard architecture) and that any inconsistencies in Customer Data are appropriately cleansed before such data is inputted into the Unit4 SaaS.

11.2 Data backup

Transactional data is backed up with retention of 7 days. Non-transactional data (e.g. documents) are kept in encrypted storage account and in Production Environment transactional and non-transactional data are replicated to the secondary location. There is no "forgiveness" restore option available. Access to the backups is limited to the Global Cloud Operations engineers in case of Disaster or malfunctioning of hardware/software. Backups are done with frequency to support RPO on level of 1 hour.

Unit4 performs the backup with frequency that supports Disaster Recovery objectives.

11.3 Data Security

Data in transit

Customer data in transit over public networks is protected with TLS 1.2.

Customer Data at rest

Transactional and Non-transactional data at rest will be secured by Standard Symmetric Encryption (AES).

11.4 Limits and regulators on usage

Unit4 runs in a Multi-Tenant environment and, as such, Unit4 observes fair use limits so that runaway processes do not monopolize shared resources. When a limit is exceeded, corrective measures will be taken.

For actual usage limits please see Fair Usage Policy at www.unit4.com/terms.

11.5 Access to my data

The Customer's Data is owned and controlled by the Customer and in accordance with Applicable Law, Customer shall be the data controller. Unit4 is the data processor.

To ensure the Customer has access to their Customer Data, the following options are available:

- Application functionality (e.g. Web Client, Mobile Applications);
- APIs/web services;

- Unit4 Extension Kit;
- Upon Agreement termination Customer Data can be retrieved by Customer in accordance with the Agreement.

11.6 Data availability to support Unit4 TM

Obfuscated copy of production made every 24 h for the purpose of support and R&D diagnostics.

11.7 People Platform Services

Unit4 People Platform Services are Multi-Tenant, shared Services. Except where explicitly stated in the Service's Service Description, each Unit4 People Platform Service has a Preview instance and a Production instance. Given the foundational nature of the Unit4 People Platform Services, Releases of Unit4 People Platform Services occur more frequently than end User facing aspects of Unit4 business solutions. Unit4 People Platform Service Releases are deployed in a transparent manner and result in no downtime. As such, Unit4 People Platform Service Releases can be deployed outside of Planned Maintenance windows. In rare cases when downtime is necessary, the Release will be performed during a Planned Maintenance window. Details regarding People Platform Services can be found in Unit4 People Platform Service Description at www.unit4.com/terms.

Glossary and Technical Acronyms

Unless defined in the tables below, capitalised words and phrases have the meaning given to them in Unit4's General Terms of Business or Unit4 Support Terms (found on www.unit4.com/terms).

Glossary

Term	Definition
Account Administrator	an appropriate and qualified Business User who will have administrative level control for creation, maintenance and deletion of Accounts providing access to the Unit4 Product.
Customer ID code	a unique Customer identifier.
Multi-Tenant	a single instance of Unit4 SaaS including its supporting infrastructure which serves multiple Customers.
Record	a data record stored within a Customer's database (for example a line in a timesheet).
Transaction	the creation or modification of a Record.

Technical Acronyms

Acronym	Full Name
ADFS	Active Directory Federation Services
AES	Advanced Encryption Standard
API	Application Program Interface (e.g. web services)
HTTPS	Hypertext Transfer Protocol Secure
Kbps	Kilobits Per Second
KPI	Key Performance Indicator
NPE	Non-Production Environment
PE	Production Environment
SHA-2 RSA	Secure Hash Algorithm (number 2) and RSA encryption Algorithm
SLA	Service Level Agreement
SOC	Service Organization Controls
TLS	Transport Layer Security Encryption