UNIT4
In business for people

Unit4 FP&A

Cloud Service Description

VERSION 1.5

June 2021

CONTENT

1. Introduction

Unit4 Financial Planning and Analysis (Unit4 FP&A) delivers financial performance management technology with native integration to Unit4's People Experience. Built on a highly flexible platform, Unit4 FP&A models are adaptable to various FP&A, Corporate Performance Management (CPM) and analytics use cases. The solutions give business Users the platform and tools they need to configure their planning and reporting to meet individual requirements, without having to have a technical background.

Unit4 FP&A provides comprehensive capabilities for supporting top-down, bottom-up and mixed planning processes across an organisation. Unit4 FP&A also offers predefined best practice models (e.g. Integrated Financial Planning, People Planning and Analytics, Consolidation) as well as industry models that can be reused and adjusted to the Customer's requirements. The purpose of this document is to describe the cloud Service composition provided to the Customer.

Unit4 provides a complete technically-managed solution for Unit4 FP&A 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 of 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 FP&A is available as a shared option (default), where computing resources are shared between Customers without any interference and a dedicated option (on Microsoft Azure only) where some computing resources are dedicated to a single Customer.

In summary, Unit4 provides the following:

- Access to Unit4 FP&A Desktop Client (RichClient), Web Client (OneClient) and API/web services;
- All User access to Unit4 FP&A is over secure internet connections (HTTPS). A variety of browsers are supported;
- Comprehensive integration options available, including the use of Unit4 APIs/web services;
- Infrastructure is fully scalable, in a high availability environment with redundancy in critical aspects such as power, hardware, network communications;
- Relevant security level;
- Continuous monitoring is in place, covering servers, Services and applications, feeding alerts and continuous improvement;
- Application of infrastructure updates, patches and hot fixes;
- Unit4 software and supporting software Releases and Hot Fixes;
- Production Environment and Non-Production Environments with a separate database for Customers' data;
- Forgiveness restores (where applicable), and disaster recovery in a physically separate secondary site;

- Service Level Agreement, with Service Credits based on Service Availability;
- Unit4 Community (Community4U) to engage with Unit4 directly, giving insight in the in Service performance indicators and see the status of Services;
- Various Azure regions leveraged to enable Unit4 to meet Customers' data residency needs; Customers' data always resides within a specified a geopolitical zone (except where explicitly stated otherwise); 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, and Nordic data center (Conapto AB) 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 Service level commitments 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 and Nordic data center (Conapto AB) details on www.conapto.se.

Geopolitical zone	Provider	Data location (Countries/City's/Regions)	Time zone
EU	Microsoft Azure	Dublin, Ireland and Amsterdam (DR), Netherlands	CET/CEST
USA	Microsoft Azure	Texas and Iowa (DR)	CST/CDT
Canada	Microsoft Azure	Quebec City and Toronto (DR)	EST/EDT
United Kingdom	Microsoft Azure	London and Cardiff (DR)	GMT/BST
Asia	Microsoft Azure	Singapore and Hong Kong (DR)	SGT
Australia	Microsoft Azure	Victoria and New South Wales (DR)	AEDT/AEST
Norway	Microsoft Azure	Oslo and Stavanger (DR)	CET/CEST

Sweden	Nordic data center (Conapto AB)	Sätra and Sollentuna (DR)	CET/CEST

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

Customer residence	**Geopolitical zone used**
APAC	Asia
Australia/New Zealand	Australia
Canada	Canada
EU	EU
Sweden	Nordic data center (Conapto AB)
Norway/ Denmark	Norway
UK	UK
US	US

In the unlikely event the primary and secondary redundancy of the network in a geopolitical zone fails, connections are rerouted using tertiary redundancy in the following way.

Primary	**Secondary**	**Tertiary**
Geopolitical zone EU	Geopolitical zone EU	Geopolitical zone UK
Geopolitical zone UK	Geopolitical zone UK	Geopolitical zone EU
Geopolitical zone USA	Geopolitical zone USA	Geopolitical zone Canada
Geopolitical zone Canada	Geopolitical zone Canada	None
Geopolitical zone Asia	Geopolitical zone Asia	Geopolitical zone Australia
Geopolitical zone Australia	Geopolitical zone Australia	Geopolitical zone Asia
Geopolitical zone Norway	Geopolitical zone Norway	TBD

3. Service model

Unit4 FP&A is available in 2 main models:

1. in a shared deployment model; and
2. in a dedicated deployment model.

Unit4 FP&A dedicated model provides the same Service offering as the shared model with the distinction that computing resources such as, SQL server are not shared with other Unit4 Customers, and are dedicated to a single Customer. The dedicated deployment option is not available for the Unit4 People Platform Services, these are always shared (Unit4 People Platform Services are Multi-Tenant).

Category	Component	Shared	Dedicated
SOLUTION	Release elasticity: Ability to defer a Release for 10 weeks (maximum)	Yes	
	All patching, updates of the standard solution (technical)	Included and automatic	
INFRASTRUCTURE	Environments included	1 Production + 2 Non-Production (Preview and Acceptance)[1]	
	Availability guarantee	Yes	
	Response time guarantee	No	
	Data centers	Microsoft Azure and Nordic data center (Conapto AB)	Microsoft Azure
SERVICES	Releases will commence	Automatically, with possibility to defer	
	On-going technical operations, performance management, maintenance of all infrastructure components,	Yes	

[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.

	monitoring alert response and issue resolution		
	Backup & Service Restore	Yes	
	Disaster recovery	Yes	
	Monitoring program of infrastructure and application	Yes	
COMPLIANCE	Compliance certificates and assurance documents – Microsoft Azure	SOC1 Type II (ISAE 3402), SOC2 type II (ISAE 3000), ISO27001, ISO27017[2]	
	Compliance certificates and assurance documents – Nordic data center (Conapto AB)	SOC1 Type II (ISAE 3402), ISO27001, ISO27017[2]	

4. Environments

Three (3) environments are provided[3], 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):
  a) Preview – a Customer's Preview environment always contains the latest Releases for the Unit4 Product in use by the Customer; and
  b) Acceptance – which can be used according to Customer needs as “Test” / ”Quality” / ”Development” / ”Pre-Production”.

Additional environments can be provided at an extra charge.

Unit4 assigns to every Customer an unique Customer ID code, which is visible in various elements of the Service (including environments) and it is used for Customer identification. The MS Azure Customers ID code is a 3-character acronym and for Nordics DC Customers

[2] Unit4 FP&A 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.

[3] 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.

ID code consists of 6 digits. The Customer ID codes are created at Unit4 discretion during the early stage of the implementation and are not a subject to change.

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; there is no concept of Customer specific instances of Unit4 People Platform Services. As such, no additional instances of Unit4 People Platform Services are provided.

4.1 Production Environments

Only the Production Environment (PE) is subject to the Service Level Agreement.

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.

Definition of an NPE refresh from or to PE

A refresh of an NPE from PE is a full copy of Customer database between the environments. Refresh of the data stored outside of the database has to be explicitly specified in the Service Request.

There is no NPE refresh option for Unit4 People Platform Services.

Point in time used

The NPE refresh is from a point in time prior to the current Business Day. The specific point in time is selected by Unit4.

Frequency of NPE refresh from or to PE

Where the PE and NPE are at the same Release level or at the different Release levels, one refresh per NPE per month is included.

Additional requests will give an extra charge per refresh per NPE.

How to request a refresh?

Refreshes must be submitted to Unit4 by a Named Support Contact using a Service Request on Unit4 Community4U.

Throughput time

A NPE refresh from PE will be available for use at the start of the second Business Day following the Service Request acceptance (depends on the contracted support level).

Users accessing an NPE

NPEs are configured to handle a maximum of 15 concurrent Users.

Customer responsibilities

Customer needs to manage non-production WIP such as non-production report templates (e.g. in progress changes to financial planning report template) as refresh will replace WIP with copies from production.

What happens to the previous NPE details after a refresh?

Everything in NPE will be erased and replaced with a fresh copy from PE.

Update of an NPE to a new Release

The Preview (NPE) environment is updated as soon as a Release is available following an announcement of Unit4.

Once an NPE has been updated to the latest Release, it is not possible to move back to the previous Release.

Backups

Backups of NPE are made daily in the time zone of the geopolitical zone in use. Backups of NPE are kept for fourteen (14) calendar days.

Restores

A restore request can be made by issuing a Service Request on Unit4 Community4U. Throughput time, amount of included restores and the charge is same to a refresh of a NPE. Please note there is no Customer specific restore option for Unit4 People Platform Services.

Suspension

NPE which is not actively used will be suspended. Suspended NPE may be reactivated at any point in time. In order to reactivate suspended NPE Customer needs to initiate re-activation, which may take up to 15 minutes.

5. Reporting and monitoring

5.1 Reporting on Service Performance

Unit4 provides operational information regarding Unit4 FP&A on Unit4 Community4U. That information includes:

- Service availability;
- Scheduled maintenance (times, dates per region);
- Release information;
- 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 targets on Production Environment.

6. Releases

Periodically, Unit4 introduces new features in the Unit4 FP&A 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 Hot Fixes, as deemed necessary by Unit4 in order to maintain the existing features of the Unit4 SaaS and to maintain Service level commitments and security.

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

- Any Releases 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; are not included in the Unit4 FP&A Service and will be a subject to additional charge.
- Where any Release replaces or updates any Configuration or non-standard functionality utilised by Customer, the Customer will be required to adopt the standard functionality. Unit4 reserves the right to charge a reasonable fee to provide assistance if Customer wishes to maintain the previous Configuration or non-standard functionality.

6.1 Release deployment

Releases may take place approximately each quarter. The frequency of Releases may be increased or decreased at Unit4's discretion. Releases may take up to twelve (12) hours to deploy, resulting in the Service being unavailable for some or all of that time (such unavailability shall not be counted as Service downtime for the calculation of Service Availability). A schedule of planned deployment of Releases to the Production Environment will be published on the Unit4 Community4U. A Customer's Preview environment always contains the latest Release of Unit4 FP&A in use by the Customer. Unit4 will use reasonable endeavours to ensure that Releases will be carried out during the Planned Maintenance window.

[APPLICABLE FOR UNIT4 PEOPLE PLATFORM SERVICES]

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 changes contained in a Unit4 People Platform Service Release can be found on the Unit4 Community4U as soon as the Release has been deployed. Releases of Unit4 People Platform Services cannot be deferred.

6.2 Hot Fix Deployment

Hot Fixes are applied as deemed necessary by Unit4 in order to maintain the existing features of the Unit4 FP&A as well as maintaining Service level commitments and security.

Please note there is no concept of an Update to Unit4 People Platform Services. All changes to a Unit4 People Platform Service are considered a Release of the Service.

7. Planned and unplanned maintenance

7.1 Planned Maintenance

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

	Standard **Planned Maintenance windows (PMW)** *Releases, Hot-Fixes and Infrastructure updates*	**Additional** **Planned Maintenance windows (PMW)** *Releases*
All regions (except Azure US, Azure Canada)	12 per year, 3rd or 4th week of each month From: Sat 4PM To: Sun 4AM UTC	2 per year according to time interval specific for given region *(unless communicated otherwise)*
Regions Azure US and Azure Canada	12 per year, 3rd or 4th week of each month **Shortened PMW:** From: Sun 4AM To: Sun 11AM UTC Or **Full PMW***: From: Sat 11PM To: Sun 11AM UTC **In rare cases, when a downtime of all regions would be required*	
Nordics Data Center	weekly, once/week From: Mon 6PM to: Tue 1AM 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 in 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 the 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 Unit4 FP&A and is subject to any and all present and future Usage Restrictions of Unit4 FP&A. Customer and Unit4 must agree, prior to monitoring, on monitoring details in order to ensure that the monitoring does not interfere with the Unit4 FP&A offering and that Unit4 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 tasks and indicates Services included as part of Unit4 FP&A and tasks that are the responsibility of the Customer (or by Unit4 Professional Services at an extra charge):

Task	Included	Customer Responsibility
Project Planning		
• Publishing general availability schedule of Releases on the Unit4 Community4U	✓	
• Managing timelines, outline goals, roles and responsibilities		✓
• Business analysis and discovery		✓
• Creating test plans		✓
Release deployment in Preview environment		
• Update Preview environment with Release	✓	
• 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		✓
• 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; and
- 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 FP&A 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 Service and managing Customer's Accounts. Customer warrants that its Account Administrator(s) will maintain authority to act on Customer's behalf concerning the Unit4 FP&A, 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 in Unit4 FP&A SaaS or its Users' Accounts, and will provide all information and take all steps requested by Unit4.

9. Customisations and integrations

9.1 Customisations

Unit4 FP&A does not support any Customisations, only configuration is applicable.

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.

Integration Type	Permitted?
Integration with Unit4 ERPx, where Unit4 ERPx financial and meta data for P&L planning and reporting are extracted by Unit4 FP&A, including deep link.	Yes
Integration with Unit4 ERP 7, where Unit4 ERP 7 financial and meta data for P&L planning and reporting are extracted by Unit4 FP&A, including deep link. Remark: For integration of Unit4 FP&A with Unit4 ERP version lower than 7.5, database replica is mandatory (which may result in additional cost for Customer).	Yes
Integration with latest Unit4 Financials supported version on summary level. Push back of data to balance tables from FP&A to Unit4 Financials.	Yes
Integration with Unit4 Student Management	Yes

10. Technical operations

10.1 Printing

All printing is carried out on the client side.

10.2 Connectivity

Unit4 FP&A is accessed via the OneClient and RichClient over the public internet using an HTTPS connection (RSA 2048 bits - SHA256 with RSA and/or EC 256 bits SHA256 with ECDSA).

The Unit4 FP&A RichClient and the Microsoft Office Add-Ins needs to be installed locally on Customer's site.

Internet bandwidth suggestions*

- Unit4 FP&A OneClient – 512 Kbps per User
- Unit4 FP&A RichClient – 512 Kbps per User
- Latency Recommended: at most 50 ms

* Rough guidance only based on simulation testing. 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.

Virtual Private Network

Unit4 can provide an optional VPN (IPsec) connection as an option only for Microsoft Azure deployments.

Client device terminating the VPN connection has to fulfil following requirements:

- Be on the list of supported hardware for Route Based VPN: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-devices
- Support Network Address Translation (NAT) to limit the networks on Customer-side to one network with maximum 24-bit mask
- Provide, at minimum, support for VPN settings listed below:

IKE version	IKE v2
IPSec Keying Mode	PSK
IKE Phase 1 – Encryption Algorithm	AES 256
IKE Phase 1 - Authentication	SHA 256
IKE Phase 1 – DH Group	At minimum DH14
IPSec Phase 2 – Encryption	AES 256
IPSec Phase 2- Authentication	SHA 256
IPSec Phase 2 – PFS Group	At minimum DH14

For Unit4 FP&A interfaces, following connectivity is available:

- One Client: exclusive to Internet, exclusive to VPN or available from both Internet and VPN;
- Rich Client: exclusive to Internet, exclusive to VPN or available from both Internet and VPN;
- SFTP access: exclusive to Internet or available from both Internet and VPN.

10.3 Technical overview

Topic	Description
FTP	
Protocol	SFTP (SSH FTP) protocol is used
Credentials	Two sets of credentials are provided per environment (e.g. 2 username/passwords for production, 2 username/password for each NPE)
Email	
Domain	Unit4 FP&A needs an SMTP Server to send eMails. By default, Unit4 mailsystem can be used, but the sender email address is limited to noreply@FP&A.cloud. Optionally the Customers SMTP Server can be used.
Protocol	SMTP over TLS
Authentication	
Protocols supported	By default, authentication for Unit4 FP&A (OneClient) is carried out using application-based username and password authentication. Management of users and passwords within Unit4 FP&A application is the responsibility of the Customer. Unit4 FP&A supports authentication via Unit4 Identity Services (IDS). IDS is a federated authentication gateway, authentication is performed at the Customer's own IdP Unit4 IDS supports WS-Federation, SAML-P and OpenID Connect support (see Unit4 IDS Service Description).
Internet communication	
Protocols supported	HTTPS secured with TLS with RSA SHA256withRSA encryption and/or EC SHA256 with ECDSA

11 Data considerations

11.1 Transfers of Customer Data to Unit4 FP&A

Unit4 deploys standard architecture and therefore, where Customer is an existing Unit4 Customer, it 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.

When Customer requests to copy a database snapshot from outside of Unit4 Cloud environment then it should be free of any Customisation objects. These objects should be sent in a separate Service Request and will follow standard Customisation review process.

11.2 Backup and Service Restore

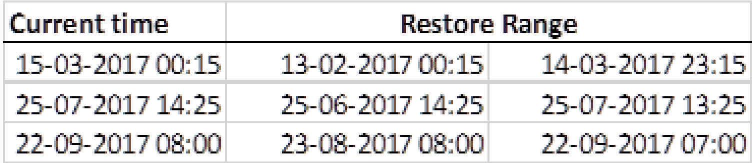
Customers are given the option of a “forgiveness” restore, where a recent Production Service backup can be restored to the PE in case of a disastrous User mistake (e.g. running month end processing in “live” environment instead of in “preview” as intended).

Backups are performed to allow for forgiveness restores to be completed with a restoration point as shown below and no later than thirty (30) days prior to current time, to a resolution as shown below. Forgiveness restores should be initiated as a P1 incident and time to complete depends on data volume.

There is no “forgiveness” restore option for Unit4 People Platform Services.

Request restore point permitted
between 1 hour prior to the time the request is made and no later than 30 days prior to the time of request to a resolution of 5 minutes

Customer may request a Service Restore report no more frequently than once per month via the Unit4 Community4U using a Service Request. Example:



Current time	Restore Range	
15-03-2017 00:15	13-02-2017 00:15	14-03-2017 23:15
25-07-2017 14:25	25-06-2017 14:25	25-07-2017 13:25
22-09-2017 08:00	23-08-2017 08:00	22-09-2017 07:00

11.3 Data Security

Data in transit

Customer Data in transit is protected with latest TLS encryption levels.

Customer Data at rest

Except for Unit4 FP&A SaaS Dedicated and cloud delivery in the Nordic data center (Conapto AB), data at rest is protected using transparent, whole database encryption (e.g. transparent data encryption, and/or whole disk data encryption). When selecting Unit4 FP&A SaaS Dedicated or deployment in the Nordic data center an extra fee will be applied to have whole database encryption. Please see the Unit4 Information Security Policy, which is available at www.unit4.com/terms.

Whitelisting

IP Whitelisting is offered as an option that will come at an additional cost in the Unit4 SaaS, as a means to gain an extended level of control on who has access to their environment. An IP whitelist is a list of IP addresses that are granted access to a certain Service. When an IP whitelist is used, all IP addresses are denied access, except those included in the IP whitelist.

IP whitelisting is available for the following product – data center – cloud type combinations.

Whitelisting	Product	Data center	Cloud Type	Available?
Web endpoints	U4FP&A	Azure	All	Yes
Web endpoints	U4FP&A	Nordic	All	Yes
When using People Platform Services whitelisting will not work due to dynamic URLs.				

Customer needs to provide VPN access to their own network for partners or Unit4 consultants working off network (to allow remote working).

The People Platform Services like Unit4 Identity Services, Unit4 Wanda and Unit4 Extension Kit use dynamic IP addresses, therefore IP whitelisting is not supported for any combination of Global products with any People Platform Services.

11.4 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:

- Unit4 FP&A (OneClient), accessed via a supported web browser;
- Unit4 FP&A (RichClient), can be setup locally (setup files can be requested via support portal.

11.5 Non-Production Environment with production specifications

As an additional Service against additional costs it is possible to opt for a Non-Production Environments (NPE), that holds the characteristics of an NPE as described in paragraph 4.2 with Production alike specifications.

11.6 Data staging area

Staging database is a separate Service provided based on the Microsoft Azure SQL database engine. That database can be used for storing any kind of staging data, no backup Services are included. The database will be open to access for uploading to and downloading from Unit4 FP&A.

Security:

Connection is secured via TLS and firewall rules that limit connectivity by IP address. Firewall rules are maintained by Unit4 and each change must be requested via Service Request in support portal.

Size(performance):

It is offered as a separate single database for each environment (see section 4.) with 50 database transaction units (DTUs) and 250GB storage included.

User Management:

Unit4 offers the database and the necessary access and credentials to work with this database. One administration account will be created and credentials will be shared with a Customer. The Customer can create more Users, if required. SQL database User management is a Customer responsibility.

SCHEDULE A
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-and-conditions).

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	An unique Customer identifier.
Customisation Object	the product of any Customisation being any code change (for example AG16 or ACT) or other database object not created using the changing of standard Unit4 Product menus and functionality.
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).
Service Restore	the time it takes Unit4 to perform the restoration of a recent Production Environment back-up (at the request of the Customer).
Transaction	the creation or modification of a Record.

Technical Acronyms

Acronym	Full Name
ACT	Advanced Customisation Tools (Unit4 ERP only)
AES	Advanced Encryption Standard
API	Application Program Interface (e.g. web services)
ERP	Enterprise Resource Planning
FTP	File Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
Kbps	Kilobits Per Second
NPE	Non-Production Environment

Acronym	Full Name
PCI DSS	Payment Card Industry – Data Security Standard
PE	Production Environment
SFTP	Secure File Transfer Protocol
SHA-2 RSA	Secure Hash Algorithm (number 2) and RSA encryption Algorithm
SLA	Service Level Agreement
SOC	Service Organization Controls
SQL	Structured Query Language
TLS	Transport Layer Security Encryption
URL	Uniform Resource Locator (a web address)
VPN	Virtual Private Network
WIP	Work In Progress