# ERP-APPS

# ERPPortal

# SaaS Service Description 2026

## Classification: Public

**ERP-APPS LTD**
*International House*
*12 Constance Street*
*London*
*E16 2DQ*
**Registered Company #** *13186463*

## Contents

# 1 Overview

ERP-APPS ERPPortal is a SaaS based product designed to enable third party users (Suppliers, Customer, People and Form Users) interact with the customers Unit4 ERP / ERPx system in specific predefined ways.

The system provides a web front end which allows these entities to undertake tasks such as:

- View and amend their Masterfile details (with standard workflow approval in the underlying ERP)
- View their transactions, payment plans and documents attached to their Masterfile
- View, acknowledge and confirm purchase orders
- Flip PO to an electronic invoice which is automatically registered in Unit4
- Submit free invoices or credits which are automatically registered in Unit4
- Make card / bank payments against invoices, on account or direct to GL using a number of payment providers, individual customers may be linked to different payment providers. (PCI-SAQ-A-EP)
- The Enterprise Web Capture portal allows you to expose and customise Unit4 forms to the web for users to complete.

The purpose of this document is to describe the cloud service provided to the Customer.

ERP-Apps  provides a complete technically-managed solution for the portal, 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.

ERP-Apps offers the solutions as Software as a Service delivery model deployed on Microsoft Azure datacentres. This model leverages Microsoft's scale and experience of running highly secure and compliant cloud services around the globe. The Azure infrastructure is excellent 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. More details can be found on the Azure Platform:

**Microsoft Azure standards compliance (e.g. ISO 27001 etc)**
https://learn.microsoft.com/en-us/azure/compliance/offerings/

**Microsoft Azure tenant segregation**
https://learn.microsoft.com/en-us/azure/security/fundamentals/isolation-choices

**Microsoft Azure encryption at rest**
https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest

**Microsoft Azure data management lifecycle (including disposal of old hardware)**
https://learn.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data
https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-bearing-device-destruction

**Microsoft Azure physical security**
https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security

ERPPortal is only available as a shared option, where compute resources are shared between customers and external users have a single account to log into multiple organisations, this is by design to help improve the experience for external users.

In summary, ERP Apps provides the following:

- Full deployment of ERP Apps Products into our cloud environment, including any required administration
- All user access to the ERPPortal is over secure internet connections (HTTPS). A variety of browsers and mobile platforms are supported. Entra authentication can be implemented where the end users are inside the Customers authentication structure for example university students (customers) having network identifications.
- All communication between the ERPPortal and the Customers Unit4 ERP system is over secure internet connections (HTTPS) using basic authentication or Unit4 IDS as standard, however other authentication methods may possibly be added on request.
- Infrastructure is fully scalable, in a high availability environment with redundancy in critical aspects such as power, hardware, network communications.
- Firewalls, anti-virus and access controls.
- Continuous monitoring is in place, covering servers, services and applications, feeding alerts and continuous improvement.
- Application of all updates, patches, hot fixes to the software.
- Production and non-production environments with a separate database for each environment.
- Disaster recovery in a physically separate secondary site.
- Formal policies in place for information security, data processing, disaster recover, business continuity and acceptable/fair use.

# 2 Data centres & data residency

ERP-Apps use the Microsoft Azure infrastructure to deliver the ERP-Apps Portals.

Various Azure regions can be leveraged to enable ERP-Apps to meet your data residency needs; your data always resides within a specified a geo-political zone (except where explicitly stated otherwise).

Note that availability in a region is not guaranteed and there may be additional costs if you want the solution hosted in a region not currently listed below.

Regular DB backups are held by Microsoft Azure for service-recovery purposes, and to recover from any application errors which may occur.
Last resort data backups are held separately in AWS cloud storage and synced daily, to ensure we can redeploy with minimal data loss should a host failure occur at an organisational level.
Data backups are held for a maximum of 31 days.

| Geopolitical zone | Primary Data Centre | DB Data Centre |
|---|---|---|
| United Kingdom | Microsoft Azure UK-South | AWS EU West 2 (London Region) |

# 3 Service Model

| Category | Component | Comments |
|---|---|---|
| Solution | All patching and updates of the standard solution | Included and automatic |
| | Environments included | 1 Production + 1 Non-Production (Stage) |
| Infrastructure | Data Centres | Microsoft Azure |
| | Updates will be applied | Automatically |
| | Ongoing maintenance and performance management of all infrastructure components | Yes |
| | Backups | Yes |
| | Disaster Recovery | Yes |
| | Monitoring of infrastructure and application | Yes |
| | Availability guarantee | Targets as standard.<br><br>Guarantee's may be provided at additional cost. |
| Compliance | ERP-Apps Compliance (Compliance of Azure host noted above) | PCI SAQ-A-EP Compliant<br>Cyber Essentials Plus |
| Helpdesk | Incident Support | Second line support will be provided by the reseller.<br>A third line support service is provided to resellers and **is not directly available to Customers**. ERP-Apps business hours are Monday – Friday 0900-1730 UK local time, excluding Bank Holidays. |

# 4 Environments

ERPPortal is only available as a shared platform option, where compute resources are shared between customers and external users have a single account to log into multiple organisations, this is by design to help improve the experience for external users.

Each customer will be provided with two environments within the shared option:

- A production environment which should be linked to the Customer's production ERP system for day to day live operations
- A Non-Production environment which should be linked to one of the Customer's non production ERP systems. Note that

# 5 Customer Responsibilities & Obligations

## 5.1 Technical & functional responsibilities

Technical Environment responsibilities:

- Supply, administration and maintenance of customer-side client devices including the Unit4 ERP environment.
- Customer-side networking infrastructure, including connectivity to the ERPPortal Service.
- Security of customer-side network, devices and internet connectivity.
- Ensuring sufficient internet bandwidth
- Customer is fully responsible for the configuration and administration of the functional aspects of the Service, including but not limited to
    - Configuration of the Unit4 ERP application, although consultancy services can be provided.
    - User administration within Unit4 ERP and the ERPPortal
    - Configuration of the connection between the Unit4 ERP Systems and the ERPPortal
- If the contract comes to an end, or the ERPPortal service is no longer in use, the customer should follow offboarding procedure as per section 10.

## 5.2 Account Set-up

Customer is responsible for designating its Users, and for ensuring that all Users are adequately trained and understand Customer's access and use obligations and requirement to comply with ERP-Apps's acceptable use policy. Where applicable each individual User must establish an Account. Customer is responsible for managing its Accounts and disabling a User's Account when ERPPortal 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.

## 5.3 Account Administrator

Customer will designate one or more Account Administrator(s). The Account Administrator(s) responsibilities include, but are not limited to, coordinating with ERP-Apps and Re-Seller support teams regarding the ERPPortal and managing Customer's Accounts. Customer warrants that its Account Administrator(s) will maintain authority to act on Customer's behalf concerning the ERPPortal

Service, and that ERP-Apps can rely on the Account Administrator(s) actions and instructions in connection therewith.

## 5.4 Account Security

Each User is responsible for keeping his or her Account credentials confidential. Users may not share Account credentials. The Customer will notify ERP-Apps immediately upon discovering any known or suspected unauthorized access to, misuse of, or breach of security for the ERPPortal or its Users' Accounts, and will provide all information and take all steps requested by ERP-Apps.

### 5.4.1 Passwords

We use a package based on industry standards to test the password strength as the user sets it. Length is more important than complexity and by using words rather than random characters it is easier to remember. There is a good summary of the latest NIST guidance here: https://www.netsec.news/summary-of-the-nist-password-recommendations-for-2021/

The user will receive a welcome email when the client add them to the portal to the email address you specify, this will give them a 24hr link to set up their own password (with the complexity set as above). If that expires then they can use the reset password function which sends a link which is valid for an hour.

Passwords are never stored in any data storage, but are hashed using an industry-recommended one-way hashing mechanism. This will be kept up to date as technology changes.

### 5.4.2 2FA

We use Google's 2FA on the back end. This can only be switched on by the client at the organisational level so all users must use it. Users may choose any 2FA application.

### 5.4.3 Single Sign On

Single sign on is possible with our Integration Pack. Currently we support Azure AD. Other authentication methods may be developed on request however there may be a charge for this depending on the requirements.

### 5.4.4 GDPR

To meet GDPR requirements users are able to delete themselves from the portal.

# 6 Reporting and monitoring

## 6.1 Reporting on Service Performance

ERP-Apps provides operational information regarding the ERPPortal on the ERP-Apps status page located at https://ERP-Apps.statuspage.io

The information includes:

- Service availability of both our services and our data centres
- Scheduled maintenance information
- Release information and deployment schedules.
- Incidents overview.
- DR status in the event it is required

All customers are encouraged to sign up to notifications on this page.

## 6.2 Monitoring program

We actively monitor our infrastructure and logs for averages and variation in application response times, infrastructure response times, outage detection, application response codes and a variety of other metrics via specifically configured dashboards.

We have a secondary active monitoring process which automatically scans these logs and metrics for critical or unusual activity and alerts the nominated person-in-charge via direct-messaging software

## 6.3 Access monitoring

In addition to our application and performance monitoring, we have detailed audit logging available so that we can track internally who has made what changes. This enables us to audit changes in the event of an incident and ensure access control policies are being enforced correctly. It also works with our defence in depth policy to provide an additional layer of discovery opportunities should any external actors gain administrative access.

# 7 Patching Policy

## 7.1 Change management and feature development process.

As an agile technology SaaS vendor ERP-Apps ERPPortal is maintained via a structured “sprint release” process on a weekly basis. These sprints will include fixes and developments and will be run in accordance with our defined Software Development Lifecycle.

Each change is initially considered based on user requirements, before going through a technical feasibility and security assessment. After planning completes the feature is added to a sprint, either in whole or in part.

At the completion of each sprint a release is automatically packaged and then pushed to an internal development environment to be tested for functionality and security. Upon completion of testing, we manually deploy the finished release to stage and production. Some larger releases may be pushed to the stage environment with a delay before being deployed to production.

Testing at each stage is a mix of automated testing, scripted testing and ad-hoc test depending on the changeset. Tests are focussed primarily on functionality and security, but also touch upon performance and reliability impacts.

For each change, code cannot be deployed without being committed to change-tracking software so that we can always roll back to a previously deployed codebase.

## 7.2 Application Releases and updates

Most of our updates are also installed “hot”. When there is a need to apply an update that has any risk of service disruption, these are scheduled into a “Planned Maintenance window” which will be out of working hours, typically on a Sunday evening.

As part of regular maintenance ERP-Apps will apply updates and bug fixes, as deemed necessary by ERP-Apps in order to maintain the existing features of the ERPPortal 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) ERP-Apps consultants; or (iii) approved reseller partner consultants, which are not included in the ERPPortal Service and would be chargeable.
- Where any Release or Update replaces or updates any Customisation or non-standard functionality utilised by Customer, the Customer will be required to adopt the standard functionality. ERP-Apps reserves the right to charge a reasonable fee to provide assistance to the Customer to the extent any such Release or Update replaces or updates any Customisation or non-standard functionality utilised by Customer and Customer wishes to maintain the previous Customisation or non-standard functionality.

To protect the Portal systems from known vulnerabilities, security patches will be deployed in a suitable time frame. Patches should be deployed as per the following schedule:

| **Vulnerability Level** | **Full deployment within (working days)** |
|---|---|
| Critical | 7 |
| High | 7 |
| Medium | 21 |
| Low | 28 |

Where the deployment of ‘Critical’ or ‘High risk’ security patches within 7 days is not possible, either appropriate compensating controls or a temporary means of mitigation will be applied to reduce the exposure faced by the Customers IT systems.

## 7.3 Unplanned Preventative Maintenance

ERP-Apps may carry out Unplanned Preventative Maintenance if there is an urgent requirement to secure the stability of, or the security of the ERPPortal Service. This action may be taken at the discretion of ERP-Apps 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 and will be reported on the status page.

# 8 Data Considerations

The ERPPortal has been designed to store as little data as possible, however there are instances where data needs to be retained in the portal.

The portal holds:

1. Portal configuration

   a. Your API, webservice URLs and any sftp / azure / email details to receive supplier invoices, payment provider details for customer portal

   b. The usernames and passwords for the above

2. Account details

   a. The name, username and email address set up in the portal for the user, the user that created them and when and their last login timestamp. This data may be downloaded by administrators in csv format.

3. Logging information

   a. We log that users have logged in and when, that they have made a change / payment / uploaded an invoice (but not the details unless there is a failure) and that they have run enquiries.

   b. We do log the IP address the requests have come from.

   c. Our logs are cleared every 30 days, the exception is customer payment logs which are retained for 90 days for troubleshooting.

   d. If you require detailed logging then the system can be configured to write detailed information back to Unit4 ERP but it will still not be stored on our servers beyond 30 days.

   e. We store server-level event logs, performance logs and error logging for admin review. For compliance reasons, these logs remain in storage for one year before being auto-deleted. We take care to ensure that no PII is stored in these logs except for remote IP addresses.

4. Redis Cache

   a. Commonly requested objects are cached in redis for between 5 minutes and an hour, depending on computational expense and data sensitivity. This cache can be cleared by administrators, users are able to clear their own personal cache.

5. Usage information

   a. We store the number of API calls made to third parties (where it is a part of a chargeable pack or has a fair use policy) in order that you can monitor this.
   b. We store single use forms' client, attribute id and attribute value so that they cannot be submitted again, we do not store the data.
   c. We store payment metadata for 90 days for monitoring and traceability.
   d. We store metadata about file uploads for 30 days for monitoring and traceability.
   e. We store metadata about invoice submission for 30 days for monitoring and traceability.

6. Temporary data in progress

a. Data input to forms:
    1. When users are inputting form data to a single stage form we pass this straight to Unit4 ERP and do not store it.
    2. When users need to be redirected away from the platform mid-form (e.g. for bank validation) and complete their form submission on return we will write the data to our database and delete it on a successful submission.
    3. When users have been redirected away from the platform mid-form (e.g. for bank-validation) and do not return, that data remains for them to resume for seven days and is then auto-deleted.
b. Files uploaded to the platform:
    1. When users upload a file as part of a form submission, or as supporting evidence to an invoice, we have to maintain this file until the primary data (form or invoice) is written to Unit4 ERP. Once written, we then attach the file to the ERP entry and delete the temporary file.
    2. If a user uploads a file and fails to complete the form or invoice submission, files are automatically deleted after seven days.
    3. If a user uploads a file, completes the primary submission (form or invoice) and attaching the file fails, we make that file available to organisation administrators to manually download and attach to the ERP record where needed. These files remain available for 30 days.
c. CSV Downloads
    1. We have functionality which allows users to download transaction information to a CSV file. As this file can be a significant size, we assemble this CSV asynchronously and notify on completion. These files are then available for download by the requesting user only for 30 days.

All other information is read / written to Unit4 ERP "on the fly"

## 8.1 Data read from ERP

The data read from ERP will depend on the portals being used by the customer. The data within each endpoint can be controlled by applying data control to the user if required, however the customer should test that this does not impact on the portal functionality.