FCO SERVICES

Part of the Foreign and Commonwealth Office

Service Description

Cirrus360 *Plus*

Cirrus360 *Collaboration*

Contents

1 Introduction 4
2 About Cirrus360 4
3 FCO Services cloud solutions 5
4 Service Description 6
4.1 Service overview 6
4.1.1 Microsoft Office Web Applications 7
4.1.2 Cirrus360 Plus and Cirrus360 8
4.1.3 Cirrus360 Remote Administration 8
4.1.4 Cirrus360 Identity Management Services 9
5 Service Management 9
5.1 Service Operations 9
5.1.1 Event Management 10
5.1.2 Incident Management 10
5.1.3 Major Incident Management 10
5.1.4 Request Fulfilment 11
5.1.5 Problem Management 12
5.1.6 Change Management 12
5.1.7 Configuration Management 12
5.1.8 Capacity Management 12
5.1.9 Availability Management 12
5.1.10 Global Support Centre 13
5.1.11 Service Delivery Manager 13
5.2 On-boarding 13
5.3 Off-boarding 14
5.3.1 Data extraction/removal: 14
5.3.2 Extraction and Return of Customer Data 14

5.3.3 Information Principles for the UK Public Sector 14

5.4 Training 15
6 Licensing Requirements 16
7 Pricing 16
7.1 Purchase Options – Pricing Overview 16
7.2 On-boarding Fee 16
7.3 Purchase Options –pricing overview 17
7.4 On-boarding Fee 17
7.5 Service Components – Functionality Overview 17

7.5.1 Cirrus360 17

8 Termination Terms 19
8.1 Termination by Customers 19
9 Purchasing, Ordering and Invoicing 19
10 Optional services 19
10.1 Service Delivery Management 20
11 Abbreviations 20
12 Legal 22
13 Terms and Conditions 22

1 Introduction

Your trusted in-government partner for secure digital solutions

The public sector is dynamic. The current threat level in the UK is SEVERE. The impact of UK's exit from EU is still largely unknown and the uncertainty which we face is comparable to the 2008 financial crisis. However, security will remain centre stage and the need for departments to transform their technology will be greater than ever - to confidently employ identity management and make full use of proprietary datasets in a secure cyber environment, which can be shared as broadly as required within the department and its agencies; to embrace the power of big data analytics for improved decision making and outcomes; and to utilise the Internet of Things (IoT) technology to drive efficiencies in areas such as preventative maintenance.

FCO Services, part of the Foreign and Commonwealth Office, works with departments to deliver secure, on government premises, UK hosted, end to end ICT services for Whitehall and overseas. Our DV/SC security cleared team have an instinctive understanding of civil servants, front and back end transformations, private cloud hosting, security operations centres (SOCs), biometrics authentication and data handling at all Security Classifications and privacy markings. With an agile global network and local, expert teams we are ideally positioned to offer trusted consultancy, professional services and managed services to customers where security and speed of response is essential.

2 About Cirrus360

Cirrus360 is a cloud-based version of familiar Microsoft productivity and software that is accessible through FCO Services' accredited PSN Protected cloud environment and is capable of operating wholly online or in conjunction with on-premises services.

Available to any government department on the Public Services Network (PSN) at PSN Protected, Cirrus360 provides Microsoft Office web applications & SharePoint. Cirrus360 enables Authorised Users to work anytime and anywhere on information across the PSN Protected network. Cirrus360 offers interoperability with software already in use and maintains a high level of efficiency through the transition to new services as Authorised Users do not have to learn how to use different applications.

Switching to FCO Services' accredited cloud with Cirrus360 will deliver low operating costs with predictable, utilisation based pricing that includes access to the latest version of applications at no additional cost.

In short, Cirrus360 provides an alternative to traditional on-premise IT services by making best use of Private cloud technologies to reduce operating and deployment costs and improves the quality of the service provided to Authorised Users.

FCO Services takes Green IT seriously and holds Participant status for the EU Code of Conduct for Data Centre Operations. As a participant, FCO Services has committed to reducing its carbon footprint, providing energy reporting and the implementation of certain practices from the Best Practice guide. Reporting forms containing energy metering data, and

information on best practice compliance status, are submitted annually to the Code of Conduct Secretariat which reviews activities and progress in meeting stated commitments.

3 FCO Services cloud solutions

- **Cost efficient** Cirrus360 allows organisations to introduce greatly improved productivity and tools by using existing infrastructure to access cloud services without the costly and complex refresh programmes that are required in traditional IT
- **Shared service** Cirrus360 is less costly to operate than traditional IT services because it is delivered from a shared services facility that already supports many Government organisations and thousands of Government users
- **Price Transparency** Pricing for Cirrus360 is based on a published table of charges per Authorised User
- **Secure** Cirrus360 has been accredited by FCO Services at OFFICIAL. The scale of Cirrus360 makes possible the use of technologies and monitoring services that may not be affordable with smaller, individual installations
- **Private Cloud** Cirrus360 is delivered through a private cloud on PSN Protected hosted at our secure UK Government site.
- **Reliable** The platform and application architecture delivering Cirrus360 has high resilience built in and it is operated from two locations with separate network connections and power supplies. Authorised User devices can work offline with subsequent synchronisation
- **Flexible** Cirrus360 can be deployed purely as a cloud-based service with data hosted by FCO Services or it can integrate with existing services and data. Cirrus360 is able to use single sign-on with on-premise services
- **Evergreen** Cirrus360 services will be updated to the latest versions of Microsoft applications at no additional cost and without the complex migrations that characterise traditional IT
- **Cross-Boundary** Many IT services cannot be shared across organisational boundaries and this limitation impedes with stakeholders and partners; Cirrus360 can be accessed across PSN Protected and is not constrained by the boundary of the organisation. Users from other organisations can be given secure permissions to share clearly defined and
protected data sets.

In Summary

- All Staff are SC or DC cleared
- UK Government grade cyber defence of digital and physical assets
- Proven track record of successfully delivering secure cloud solutions
- All services aimed specifically at UK Government requirements
- Collaborate securely across boundaries
- Quickly adopt the service as Authorised Users are familiar with Microsoft applications

4 Service Description

4.1 Service overview

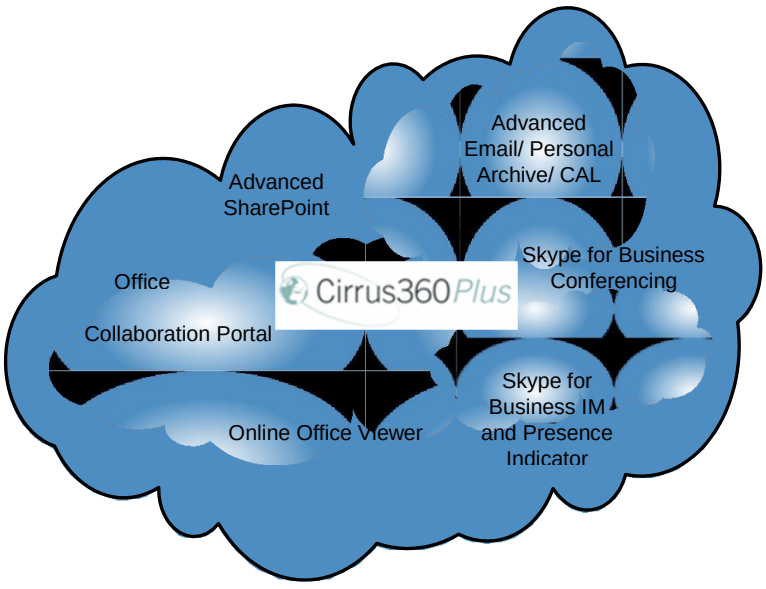
Cirrus360 is an FCO Services Protected cloud service for organisations of all sizes. Instead of installing and deploying Microsoft SharePoint Server on-premises, any organisation can now simply subscribe to Cirrus360 to provide a high grade solution for creating sites to share documents and information, and to collaborate effectively with colleagues and partners over the PSN. Hosted on FCO Services' established PSN Protected cloud platform, organisations can take advantage of sophisticated capabilities without the operational burden and associated costs of on-premises servers.

Cirrus360 helps organisations of all sizes to:

- **Work together effectively** Share documents and track project milestones to keep all parties aligned.
- **Keep documents up to date** Manage important documents online so the latest versions are always at hand.
- **Easily access information online** Provide everyone in a team with access to critical business information when and where they need it.
- **Easily protect critical business information** Control which users can access, read and share documents and information.

Cirrus360 works with familiar Microsoft Office applications. It's easy to create Office documents and save them directly to Cirrus360, or co-author documents with Microsoft Office. Authorised Users can access important documents offline and set document-level permissions to protect sensitive content.

In addition, Cirrus360 makes it possible, with one click, to communicate in real-time with colleagues, customers and partners from within SharePoint sites using Cirrus360 Communicator, which is part of the Cirrus360 suite of online services.



4.1.1 Microsoft Office Web Applications

Microsoft Office Web Applications allows Authorised Users to view, share and edit documents using a PSN Protected connected device. It is possible to make simultaneous edits to files in real time whilst maintaining document fidelity and formatting even when other users are working on a different device with a different version of Office installed.

Key Features:

- **Manage Office Files** View, edit and share content created in the Word, Excel, PowerPoint, and OneNote desktop applications online, from a variety of devices.
- **Familiar Tools** A common set of online viewing and editing tools to people who use different platforms and different versions of Microsoft Office, including those who do not have Microsoft Office on their computers.
- **Familiar Features** An environment that uses many of the same editing and formatting features Authorised Users already know from using Microsoft Office.
- **Co-Editing** Simultaneously edit shared Excel spreadsheets and OneNote Shared Notebooks with co-authoring support in the Office Web Apps. See the areas colleagues are editing in real-time.
- **Email** workers in your team with the latest Outlook client and tools.
- **Communicate** using Skype for Business.

4.1.2 Cirrus360 Plus and Cirrus360

Key features of the Cirrus360 include:

- **Secure access** Cirrus360 is accessed through 128-bit Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption. Anyone who intercepts a communication sees only encrypted text.
- **Intrusion monitoring** FCO Services continuously monitors the Cirrus360 systems for any unusual or suspicious activity through its Security Operations Centre (SOC).
- **Security audits** FCO Services regularly assesses the Cirrus360 infrastructure to ensure that antivirus signatures and required security updates are installed and that high-level configuration settings comply with CESG security policies.
- **High availability** All services have a 99.9% availability target.
- **Highly Resilient** The Cirrus360 service is operated from two data-centres with multiple, diverse network infrastructure to minimise unscheduled service outages. Data-centres act as backups for each other so that if one fails, the affected customers are transferred to another data-centre with minimal interruption of service

- **Single Sign-on** the standard service offering provides a forms-based single sign-on for full access to all of Cirrus360. If required, Federated Identity Management is supported by Cirrus360. Federated Identity Management enables the sign-on to Cirrus360 to be synchronised with the existing corporate logon by configuring on- premises Microsoft Forefront Identity Manager (a separate Microsoft product) to federate with the FCO Services Cirrus360 Federation Gateway. Alternatively a Domain Trust can be configured to allow an existing corporate identity to be used to access Cirrus360 services. FCO Services Government Secure Specialist Cloud Services can provide advice on implementing and integrating these optional services as required for an additional charge.
- **Up-to-date Tools and Applications** will be updated with all relevant patches and fixes.

4.1.3 Cirrus360 Remote Administration

Many aspects of the Cirrus360 service can be configured with standard browser based administration tools. These standard Microsoft tools are designed to allow Authorised Users, power users and administrators control over the configuration of the various applications within Cirrus360.

Using Remote PowerShell, delivered to the Authorised User's desktop using Application Virtualisation Services, administrators can connect to Cirrus360 to perform management tasks that are not available or practical in the web management interface. For example, they

can use Remote PowerShell to automate repetitive tasks, extract data for custom reports, customise policies, and connect Cirrus360 to existing infrastructure and processes.

4.1.4 Cirrus360 Identity Management Services

Cirrus360 Identity Management includes the creation of Authorised User accounts, password policy, co- existence, directory synchronisation, and single sign-on (Federated Identity). Authorised Users will be able to gain access to Cirrus360 by authenticating either through a prompt to provide valid credentials or through an optional single sign-on process. Once authenticated, Authorised Users' identities refer to the Authorised User names associated with the Cirrus360 accounts.

There are two types of identities:

- **FCO Services' Online Services Cloud IDs (Cloud Identity)**: Users receive cloud credentials— separate from other desktop or corporate credentials—for signing into Cirrus360 services. The cloud ID password policy is stored in the secure cloud within the customers tenant hosting the Cirrus360 service
- **Federated Identity**: In organisations with on-premises Active Directory, there are two optional methods of using federated identity between the corporate domain and the Cirrus360 service:
    1. Configure an on-premise installation of Microsoft's Forefront Identity Manager to synchronise corporate accounts with the Cirrus360 domain. Authorised Users will still use a dedicated Cirrus360 cloud Identity to access the Cirrus360 services, but the username and password will automatically match their local corporate identity.
    2. Configure a Domain Trust between the local corporate domain and the Cirrus360 domain. This allows Authorised Users to sign into Cirrus360 services using their corporate Active Directory credentials. The corporate Active Directory authenticates the Authorised Users and stores and controls the password policy.

Full functionality of the options described above will be dependent on configuration and compatibility with Desktop Infrastructure. Implementation of Federated Identity will require use of the FCO Services' Government Secure Specialist cloud Services to work with the customer to integrate with the existing IT environment.

5 Service Management

5.1 Service Operations

FCO Services Operational support staffs ensure purchased services are managed in accordance with the agreed service offering. FCO Services aligns its service delivery to ITIL V3, ISO 20000 and ISO 9001 best practices.

This includes monitoring, analysing events, incident management and request management to ensure service targets are met. Where targets are threatened or breached problem management activities will be employed to ensure high quality service prevails. FCO Services employs a rigorous change management process to protect services whilst deploying necessary changes to the environment.

5.1.1 Event Management

FCO Services utilises a range of technology to monitor the end to end services we deliver. This technology is configured to identify potential issues around capacity and availability thresholds in order for our Subject Matter Experts (SMEs) to take proactive, preventative actions to ensure services are not compromised.

If an event is exception based, it is dealt with under our incident management process.

5.1.2 Incident Management

Incident Management is an essential process to ensure all identified or reported faults and perceived faults are resolved to our agreed, published resolution targets.

Our ISO9001 accredited process is provided by our experienced Global Support Centre and, out of core hours, our Operations Control Centre. These teams are supported by our technical SMEs.

Priority Level	Definition	Response Time	Resolution Time
Priority 1	• The entire service is unavailable due to an issue with FCO Services infrastructure • The security of the infrastructure is compromised	30 mins	4 hours
Priority 2	• Certain parts of the service infrastructure (provided by FCO Services) are unavailable, causing degradation to service	30 mins	8 hours
Priority 3	• Failure of a component supporting a service which is not adversely or directly impacting service (reduced resilience) • Risk of failure of a service (e.g., Storage utilisation increase, potential security threat identified)	4 working hours	12 hours
Priority 4	• Incident raised from a threshold alert, where sufficient time exists to prevent service unavailability or degradation • Single user issue, where normal service is available for the majority of users.	12 working hours	72 hours

P1 and P2 resolution times are applied 24x7x52
P3 and P4 resolutions are limited to UK core working hours – Mon-Fri 07:00 – 19:00 excluding bank holidays

5.1.3 Major Incident Management

In the event of a major incident, our highly competent Incident Managers co-ordinate rapid resolution through our ISO9000 accredited major incident procedure.

Major incident reports are generated for all P1 incidents and will be delivered within 5 working days after the resolution of the incident.

Major incident reports for P2 incidents can be provided on request within 10 working days and are subject to charge.

5.1.4 Request Fulfilment

The Request Management process enables FCO Services to deal with requests from the Customer in a consistent manner.

The process is provided at the front end by our experienced Global Support Centre, and out of core hours, by the Operations Control Centre.

Level	Definition	Response Target	Fulfilment Target
Level 1	• Critical request with specific time constraints agreed within the Service Catalogue. • Typical examples would be Password Resets, User Suspension, Account disables, urgent account restores. • These requests require 'pre-approval' from the customer to allow tight timescales to be met.	30 mins	4 hours
Level 2	• Important request but less time critical. Likely to cover EUD Peripherals and other important but not time critical items. • These requests require 'pre-approval' from the customer to allow tight timescales to be met and may be subject to additional costs.	30 mins	2 working days
Level 3	• Important request but less time critical. Likely to cover EUD Peripherals, adhoc reporting requests and other important but not time critical items. • These requests require customer approval prior to their initiation and may be subject to additional costs.	4 working hours	5 working days
Level 4	• Non-essential business requirements such as new standard report requests, increased capacity requests.	12 working hours	20 working days

L1 fulfillments are applied 24x7x365

L2, L3 and L4 fulfillments are limited to UK core service hours (Mon-Fri 0700 – 1900, excluding public holidays) Fulfillment time is defined as the time from receipt of the Request to it being fulfilled.

5.1.5 Problem Management

Our ISO9001 accredited problem management process is engaged after a major incident, a trend of recurring incidents or when customers or SME believe further investigation is required to determine why incidents occur.

We employ various root cause analysis techniques with our SMEs, (internal service providers, external suppliers and Customer organisations – where applicable) to identify why incidents occur and then determine the most appropriate solution to eradicate the root cause.

Where it is not possible or practical to eradicate the root cause, known error records exist for use by the first line teams or SME to provide quick fixes to known issues.

5.1.6 Change Management

Change Management ensures that any enhancements to existing services are impact and risk assessed by the relevant SME to ensure the change is necessary and to mitigate any risks to ensure a successful change without incurring unnecessary, unplanned or unexpected degradation or disruption to any of our services.

Our change process is used for service introduction, retirement, enhancements to technical products, software and patching activity.

A major aspect of our change process is ensuring timely and necessary communication with our Customers around planned and emergency change events.

5.1.7 Configuration Management

FCO Services' Configuration Management System (CMS) is used to manage and control components to provide our internal and customer facing services.

FCO Services utilise the CMS to assist with impact assessments, track license and certificate renewals and construct valid monitoring of services. The CMS is also used to determine spare stock holdings and replacement technical components and when to refresh components.

5.1.8 Capacity Management

Capacity is monitored through our event management function.

Capacity thresholds are built into event management tools to trigger capacity informational, warning or exception events which are dealt with appropriately by our SME. This could result in customers being contacted and advised of the alerts and agreeing steps to avoid service disruption together.

5.1.9 Availability Management

The Service is delivered with a target availability of 99.9%

Availability Management is supported with event monitoring and our incident, problem, change and release and deployment management processes.

FCO Services measure this using the formula:

$$\frac{\text{(Total service hours) minus (unplanned outage duration)}}{\text{Total service hours}} \times 100$$

Unplanned outages are defined as a P1 Incident. Downtime is calculated and evidence within the P1 record and associated Major Incident Report.

5.1.10 Global Support Centre

The FCO Services' Global Support Centre (GSC), is the single point of contact for the receipt of all interactions, incidents and service requests from the customer's nominated super-user. This service is available 24x7x365, supported by the Operations Control Centre (OCC) outside of core support hours.

The nominated super-user will be able to phone, email or utilise Skype for Business to contact the GSC Service Desk to raise interactions which could lead to an incident or service request.

5.1.11 Service Delivery Manager

A Service Delivery Management function provides a maximum of 2 days effort per month to each tenant.

A Service Delivery Manager (SDM) is be the point of escalation between the customer and the GSC Service Desk and is responsible for:

- Understanding the customer business and ensuring the service delivered by FCO Services is aligned to these needs.
- Managing queries outside the remit of the GSC Service Desk and the support teams
- Managing escalations.
- Assisting in costing queries for modifications to the service.

If there are instances where SDM effort is going over the included 2 days per month, FCO Services reserves the right to invoice the additional time to the customer at its then-current rates.

5.2 On-boarding

FCO Services provision the Customer's Cirrus360 tenant(s) as part of its on-boarding process. The on- boarding process involves the creation of a standard tenant environment. As part of the on-boarding activity, FCO Services works with the customer to schedule the provision the tenant(s) to the customer's configuration in line with the standard tenant architecture.

Where customers require a tenant configuration to support greater Authorised User numbers or increased storage requirements, FCO Service can provision enhanced architecture to support those specific needs.

5.3 Off-boarding

5.3.1 Data extraction/removal:

Customers have the ability to extract their data from the service at any time. Upon termination or expiration of the Customer's subscription to the Cirrus360 Service, the Customer may contact FCO Services and request that:

Their account be disabled and all data deleted (in accordance with CESG assured processes); or

The customer data is retained in a limited function for a maximum of 28 days after expiration or termination of the service so that further data may be extracted.

Note: Data can be extracted at any time prior to the expiration or termination of the subscription.

In offering Cirrus360 service, FCO Services acts as the "Data Processor" acting on the customer's behalf, and the Customer remains the "data controller". As data processor, FCO Services will only act upon customer instructions.

5.3.2 Extraction and Return of Customer Data

Upon expiration or termination of a Customer's use of the Cirrus360 Service, customers may extract their data at any time, up to a maximum of 28 days following the termination of the service agreement. As the Customer remains the "data controller" at all times, they are responsible for ensuring that they remove the content which they wish to retain.

As the Customer is responsible for the extraction of their data, there is no additional price to do so. If the Customer wishes to hire a Consultancy firm, or purchase 3rd party tools to assist with any data migration, then appropriate charges may apply with those partner entities.

Following the termination of the agreement with FCO Services, all customer data will be disposed of using CESG assured processes. FCO Services provides multiple notices prior to deletion of customer data, so that Customers are informed and reminded of the upcoming deletion of the data if they don't act within the stipulated time frame.

5.3.3 Information Principles for the UK Public Sector

The FCO Services Cirrus360 Platform supports some of the Information Principles for the UK Public Sector, in that not all principles are strictly relevant for an this offering. Specifically, the 7 Principles are supported as stated below.

Principle	FCO Services Supporting Information

Information is a Valued Asset	The Cirrus360 Platform is a resilient and fully managed hosting service with documented backup, recovery and availability procedures. All information stored in the Platform, including backups and resilient copies are located in UK Government Sites and will be protected as valued assets.
Information is Managed	All information in the Cirrus360 Platform is managed appropriately as a HMG data asset. Governance is defined and documented in the System Risk Management and Accredited Documentation Set (RMADS). FCO Services, as a Government organisation, operates its systems in accordance with all relevant HMG Information Management Standards.
Information is Fit for Purpose	All Information collected for operation of the Platform is stored and processed in appropriate formats and is necessary for platform operation and compliance with relevant regulations. Information stored by Customer using on the Platform is not modified or used by FCO Services in any way.
Information is Standardised and Linkable	Numerous Information formats and publishing methods are the supported by the Cirrus360 service. FCO Services strongly encourage customers to configure their Cirrus360 sites to support Web Standards and be deployed and published to appropriate shared service networks.
Information is Re-Used	As a SaaS system, Cirrus360 does not natively deliver on this principle. Information use and publishing are the responsibility of customers. It is not appropriate, as a service provider to re-use customer information. However, as a Shared Service Cirrus360 enables an innovative and flexible shared platform for customers to build shared services and repositories.
Public Information is Published	As a Protected platform, the Cirrus360 platform does not provide the ability to publish information to the Public. However, if appropriate, tenant applications can be constructed, with appropriate security gateways, to provide information for onward publishing.
Citizens and Businesses Can Access Information About Themselves	As a Protected platform, the Cirrus360 platform does not provide the ability to publish information to the Public. However, if appropriate, tenant applications can be constructed, with appropriate security gateways, to provide information for onward publishing.

5.4 Training

Training in the Microsoft applications is available at an additional cost as part of the qualifying Microsoft licensing agreement. Please refer to FCO Services Government Secure Specialist Cloud Services Service Definition

Additionally, migration support services are available from FCO Services to enable smooth transition into Cirrus360.

6 Licensing Requirements

The FCO Services cloud Service is based on the assumption that all Authorised Users of the Service have a Client Access License (CAL) with active Software Assurance (SA) for the appropriate workload/workloads. This pre-requisite is solely the responsibility of the end customer and active SA must be maintained on all CALs accessing the service for the duration of the term with FCO Services. If, prior to commencement of service, or at any point during the term with FCO Services, CALs with active SA are unavailable or become unavailable, then it is the end customer's responsibility to seek alternative licensing arrangements with Microsoft to ensure a compliant licensing position.

If a customer does not hold the required client licensing, FCO Services may be able to provide the required Licence compliance through a Service Provider Licensing model. Service Provider Client Licensing is not included in the base Cirrus360 pricing and price and availability is affected by the legal status of the Customer organisation.

7 Pricing

Cirrus360 Plus Price is:

7.1 Purchase Options – Pricing Overview

Cirrus360 Plus Service Components	Price Per Authorised User Per Day	Categories to which Cirrus360 Plus Service Component can be used
Cirrus360 Mail	£0.76	Please refer to Cirrus360 Mail Plus 'Functionality Overview' below.
Cirrus360 Collaboration		Please refer to Cirrus360 Collaboration Plus 'Functionality Overview' below.
Cirrus360 Communicator		Please refer to Cirrus360 Communicator Plus 'Functionality Overview' below.

Note: User counts are per Authorised User login per Cirrus360 Plus tenant.

The Price is due and payable on the date that FCO Services advises the Customer that the service is ready, regardless of when or if the Customer utilises the service.

7.2 On-boarding Fee

FCO Services will provision the customer Cirrus360 Plus tenant(s) as part of its on-boarding process. The on-boarding process involves the creation of a standard tenant environment.

Tenant Size	On-boarding Fee	Description
Standard	£5,000	Up to 5,000 Authorised Users, 24TB of mailbox storage and 2.4TB of indexed SharePoint data

The Cirrus360 Collaboration Price is:

7.3 Purchase Options –pricing overview

Service Components	Price Per Authorised User Per Day
Cirrus360 Collaboration	£0.49

Note: User counts are per Authorised User login per Cirrus360 tenant.

7.4 On-boarding Fee

FCO Services will provision the Customer's Cirrus360 Collaboration tenant(s) as part of its on-boarding process. The on-boarding process involves the creation of a standard tenant environment.

Tenant Size	On-boarding Fee	Description
Standard	£5,000	Up to 2.4TB of indexed SharePoint data

As part of the on-boarding activity FCO Services' will work with the Customer to schedule the provisioning of the tenant(s) to the Customer's configuration in line with the standard tenant architecture. Where customers require a tenant configuration to support greater Authorised User numbers or increased storage requirements, FCO Services can provision enhanced architecture to support those specific needs at additional agreed cost.

The Price is due and payable on the date that FCO Services advises the Customer that the service is ready, regardless of when or if the Customer utilises the service.

7.5 Service Components – Functionality Overview

7.5.1 Cirrus360

Feature	Cirrus360 as part of Cirrus360 Plus
Can access all team sites by default?	Yes
My Site	Yes

Enterprise Features (Access, Business Connectivity Services (BCS), InfoPath Forms, Excel and Visio Services) *	Yes
Office Web Apps	View and edit
Can be an administrator of tenant, web application, site collection and/or site?	Yes
Storage (pooled)	5 gigabytes (GB) base customer storage plus 500 megabytes (MB) per Authorised User.
Storage per external Authorised User	N/A - Cirrus360 Plus does not differentiate between internal and external Authorised Users
Additional storage	Available at a cost per 20 gigabyte (GB) block per month.
Site collection storage quotas	Up to 200 gigabytes (GB) per site collection
My Site storage allocation	Storage quotas can be set by the tenant administrator. My Sites consume the pooled storage allocation
Site collections (#) per tenant	Up to 250,000 (non-My Site collections)
Host Named Site Collections	No
Web Applications	1 (Additional web applications can be purchased if required)
Content Databases (#) per tenant	Up to 500
File upload limit	2 gigabytes (GB) per file (250 MB default)
External Users (PALs)	Cirrus360 Plus does not differentiate between internal and external Authorised Users
Microsoft Office support	Microsoft Office 2013 Microsoft Office 2010 with Service Pack 2 (with KB 2553248) Microsoft Office 2007 with Service Pack 2 (with KB 2583910) Microsoft Office for Mac 2011 with Service Pack 1
Browser support	Internet Explorer 8, 9, 10 and 11 Mozilla Firefox (latest released version) Apple Safari (latest released version) Google Chrome (latest released version)

* Requires an Enterprise CAL

Note that Cirrus360 ‘storage’ is defined as storage available for SharePoint Content Databases. SharePoint uses a number of other supporting databases and file storage (e.g. for the search index, usage analytics, etc) and sizing for these is taken into account when allocating Content Database storage based on average usage. If a customer finds the default allocation for these supporting services is not sufficient, additional storage can be purchased once the specific requirements have been captured.

8 Termination Terms

8.1 Termination by Customers

Agreement term and termination. This agreement will remain in effect unless you terminate it subject to the terms of this Section. Termination will only terminate your right to renew an existing Order or place new Orders for additional Products under this agreement. Termination will not affect any Order not otherwise terminated and this agreement shall remain in effect for such Order for the remainder of the Term.

Termination of an Order. You may terminate an Order at any time during its Term. A termination will be effective at the end of the monthly Order cycle during which you terminate the Order. You must pay for the period prior to the termination effective date.

Termination Terms by FCO Services

The following applies:

One month (“month-to-month”) Order. A one month Order may be terminated anytime without any fee

One year Order (including prepaid) under which you commit in advance to purchase a specific quantity of Products for use during a Term. You pay on a periodic basis during the Term in advance**.** If you terminate a one year Order within 30 days of the date **on which the Order became effective or was renewed**, you must pay for the initial 30 days of the Order. No payments will be due for the remainder of the Order. If you terminate an Order at any other time during the Term, you must pay 25% of the Order fee otherwise due for the remainder of the one year Term.

9 Purchasing, Ordering and Invoicing

The service can be purchased via the G Cloud Digital Marketplace framework and will be invoiced a month in arrears.

10 Optional services

FCO Services are able to offer additional services for Cirrus360, over the standard offering, at additional cost. As each customer may have differing requirements, FCO Services will provide consultancy and advice prior to provisioning.

10.1 Service Delivery Management

In addition to the maximum two days Service Delivery Management support per month, additional support can be purchased. The Service Delivery Manager (SDM) will be supported by experienced technical and service architects along with security consultants; whose services will be available as required throughout the term. They will act together as the Design Authority; to assure continued integrity of the service, to review and provide an impact analysis of proposed changes, to moderate on technical issues and to maintain design/process and technical documentation.

The following is an overview of the additional benefits a Service Delivery Manager can also deliver:

- Monthly report covering all areas of the service from Incident Management, Problem Management, Change Management, Service Level Management, Capacity Management, Availability Management Service Improvements Management. This report will be delivered by the SDM including attendance at the Monthly Service Review meetings
- Attending customer meetings in addition to the monthly service review
- Understanding the customer business and ensuring the service delivered by FCO Services is aligned to its needs
- Understand the client's needs and expectations and develop strategies to exceed and continuously improve
- To act as the single point of contact for all service related issues and provide relationship ownership and continuity service
- To identify and manage issues and risks and take responsibility for reporting issues and risks in a timely, open and appropriate manner

The Customer will make a request for SDM services through the GSC Service Desk as a service request. FCO Services will respond to this service request within ten working days. Subject to availability of qualified FCO Services resources, the parties will agree a commencement date for the SDM services.

11 Abbreviations

Abbrev.	Meaning
.pst	Personal Storage Table
API	Application Programming Interface
BCS	Business Connectivity Services
CAL	Client Access Licence
CESG	Communications-Electronics Security Group
CSIP	Continuous Service Improvement Plan
DV	Developed Vetting
FAST	Fast Search and Transfer ASA

FCR	First Contact Resolution
GB	Gigabit
HTTPS	Secure Hypertext Transfer Protocol
ID	Identification
IDS	Intruder Detection System
IE	Internet Explorer
IL3	Impact Level 3
IM	Instant messaging
IMAP	Internet Message Access Protocol
IT	Information Technology
ITIL	Information Technology Infrastructure Library
KPI	Key Performance Indicator
MAPI	Messaging Application Programming Interface
MB	Megabit
MIR	Major Incident Report
ODF	Open Document Format
OS	Operating System
OWA	Outlook Web App
PAL	Partner Access License
PC	Personal Computer
POP	Post Office Protocol
PSN	Public Sector Network
RPC	Remote Procedure Call
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SA	Software Assurance
SCOM	System Centre Operations Manager
SIE	Service Impacting Event

SIPS	Service Improvements Plan
SLA	Service Level Agreement
SOC	Security Operation Centre
SSL	Secure Sockets Layer
TB	Terabyte
TLS	Transport Layer Security
UK	United Kingdom
UPS	Uninterruptible Power Supply
WebDAV	Web Distributed Authoring and Versioning

12 Legal

See separate Terms and Conditions document.

13 Terms and Conditions

See separate Terms and Conditions document.