GovPrint Cloud Statement of Requirements

# Version Control

| **Version** | **Description** | **Author** | **Key changes** | **Date** |
| --- | --- | --- | --- | --- |
| **1.0** | **Initial version** | **Keith Houghton** |  | **01/07//24** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# PURPOSE

The Civil Service Operations Board (CSOB) agreed that departments and their Arms Length Bodies (ALBs) should adopt common property technology (PropTech) standards. CSOB mandated the Government Property Agency (GPA), hereon referred to as the ‘Authority’, to define and share PropTech standards, and departments to move towards these standards. In addition, CSOB mandated departments to work with the Authority to support an interoperable print service for government offices. This mandate has been communicated through chief operating officers.

GovPrint is part of a suite of products being delivered to support the strategic objectives mandated by the CSOB (others include GovWifi, GovPass and shared Audio Visual). The aim of these services is to create interoperable buildings that enable civil servants to work seamlessly across locations. These services also support more flexible use of buildings. Deployment of GovPrint will also support further improvements in the interoperability maturity of Authority and clients consuming these services.

GovPrint is aligned with and supports Authority's strategic objectives of:

1. Better Value - fewer printers across government that are used more efficiently
2. Contributing to Net Zero - fewer printers with lower energy use and improved recycling
3. Transforming the Civil Service - flexible and mobile working, users can print anywhere allowing them to work from any location
4. Creating a great place to work - delivering a service that meets user and client needs, simple to use with consistent functionality across all locations

Currently GovPrint can only be delivered via the Authority’s contract with Xerox which was awarded based on a further competition on Lot 2 of the CCS print framework RM6174.

With the current pipeline of known potential clients for GovPrint it is expected that the current contract will limit the addition of further clients, locations or devices beyond the next 18 months.

To support the strategic objectives for the Authority and GovPrint by continuing the deployment of GovPrint across the public sector including Authority locations there is a requirement for a scalable commercial vehicle to support this. For context there are an estimated 33K devices across the Civil Service estate that the CSOB has mandated must be supported by GovPrint, with the current Xerox contract the Authority will be limited to supporting around 2,000 devices. The number of devices that GovPrint could support outside of this mandate, across local government and central government, out of scope of the CSOB, is expected to be significantly more.

# BACKGROUND TO THE CONTRACTING AUTHORITY

The Authority exists to provide a single Civil Service general purpose estate managed for the benefit of all departments. The Authority has a 10 year strategy, covering the period 2020-30. The Authority’s Business Plan sets out the direction and purpose of the Authority. This business plan is anchored into the Government Estate Strategy with the Government Hubs Programme contributing to six out of the eight defined missions. Over this timescale the Authority expect to transform the way the general purpose government estate supports public service delivery by:

* Improving the experience of the workplace for civil servants
* Enabling increased working across departmental boundaries within the public sector
* Supporting moves from London to the nations and regions of the UK
* Taking a locality planning approach to optimise the government estate, and working with local authorities to embed our contribution to place-making
* Responding to the changes in ways of working including hybrid working
* Improving the sustainability and condition of the estate

The Authority aims to provide a single estate that brings teams together with interoperable IT will be a major enabler of transformation. To support shareable technology within hubs, the Authority is deploying a common user facing IT stack which currently comprises the following services:

* Shared Network
* GovPrint Shared Printing (GovPrint 2 / GovPrint Cloud)
* Shared Audio Visual (AV) / Meeting Room
* Digital Signage
* Shared Room Booking
* Building Occupancy Monitoring

# BACKGROUND TO REQUIREMENT / OVERVIEW OF REQUIREMENT

The Authority has delivered the GovPrint shared print service to multiple Government Departments via a contract awarded under RM6174. With the current pipeline of known potential clients for GovPrint it is expected that the current contract will limit the addition of further clients, locations or devices beyond the next 18 months.

Following the success of the current GovPrint service the Authority has reviewed the options for the ongoing delivery of GovPrint beyond the current contract. The aim was to define a strategic solution that would allow the Authority to deliver GovPrint over a longer time frame while also providing a fully interoperable service. The current model of selecting a new GovPrint supplier every 3 or 4 years will lead to multiple GovPrint services that are not interoperable.

The Authority’s long term goal has been to create a ‘GovPrint ecosystem’ of interoperable services. This would allow the deployment of interoperable services from multiple suppliers that would enable users to access print services across all suppliers systems. The Authority completed a market engagement exercise to understand whether this approach could be supported. The general consensus was that this would be technically possible but could not be delivered within the required timescales.

Therefore, The Authority’s selected strategic approach will be to split the GovPrint service into two components; Cloud and Devices, see Table 1. This approach would use the single GovPrint cloud to provide interoperability between devices from multiple hardware manufacturers.

Table 1 - GovPrint components

| **Component** | **Description** | **Procurement** |
| --- | --- | --- |
| GovPrint Cloud | Cloud print management including follow me print and scan | This procurement |
| GovPrint Devices | Catalogue of print devices (MFDs)  Cloud device management  Consumables  Deployment services  Support / Operational services | CCS RM6361 Lot 4 - GovPrint |

GovPrint Devices will be procured via a new GovPrint lot on the upcoming CCS MFD framework (RM6361) allowing contracts to be placed with multiple suppliers and devices connected to the GovPrint Cloud.

The Authority is now looking for a supplier to deliver the GovPrint Cloud, a shared cloud print management service for its future Authority hubs, other Authority locations and non Authority locations. This approach enables the Authority to have a single cloud solution that devices from multiple suppliers connect, to support interoperability between devices from multiple suppliers on the CCS RM6361 Lot 4 framework.

The Authority still wishes to move to a service delivery model based on having a GovPrint ecosystem based on interoperable print services (Cloud + Devices) from multiple manufacturers. The supplier will be required to actively support the development of interoperability between their solution and other suppliers solutions.

Delivering an interoperable GovPrint service will enable Authority to:

* Support the strategic business and IT objectives of the Authority, providing shareable technology across hubs
* Support flexible ways of working by providing a shared service for increasingly mobile users working across multiple locations
* Support the need for wider interoperability to provide shared printing across government and the wider public sector
* Support longer term goals interoperability across multiple departments
* Support the design concepts of the hubs shared network and simplifies client onboarding to the shared network
* Support the efficient and effective reduction in printing across government
* Reduce the costs for procurement and deployment of print services across government
* Reduce disruption at the end of each device contract

The aims and objectives of the GovPrint Cloud service will be to deliver a service that is:

* Cost effective with market competitive costs, the total cost of ownership for the GovPrint service must not be greater than the cost of clients providing their own print service
* Meets clients print, copy and scan requirements
* Simple to onboard clients to the service
* Flexible and can scale to meet demand
* Secure and meet all clients security needs plus aligns with National Cyber Security Centre (NCSC) guidance
* Contributes to Net Zero by reducing energy usage, CO2 reduction and increase recycling
* Contributes to Authority’s Social Value Plan currently under development

Authority will offer two main options for clients that wish to onboard to the GovPrint service as outlined in Table 2 - GovPrint delivery options.

Table 2 - GovPrint delivery options

| **GovPrint Delivery Option** | **Service Description** |
| --- | --- |
| Fully Managed GovPrint service | The client can consume the full GovPrint service including the provision of devices and connection to the GovPrint cloud utilising the Authorities contracts. |
| GovPrint Cloud only | The client can procure supported devices via CCS RM6361 Lot 4 GovPrint, or any other means the client chooses, and connect them to the GovPrint cloud. |

# DEFINITIONS

Table 3 - Definitions

| **Term** | **Definition** |
| --- | --- |
| Authority / The Authority | Government Property Agency |
| Authority Location | Other non hub Authority locations |
| BPSS | Baseline Personnel Security Standard |
| Client | Government department or agency using Authority services |
| CSIP | Continual Service Improvement Program |
| Direct Print / Push Print | User submits a print job directly to a specific Print Device and the job is printed immediately |
| EUC / End User Compute | End user compute device e.g. laptop or desktop |
| Extension Period | The optional extension periods of 1+1+1+1+1 under the call off contract. |
| Fleet / Device Fleet | Fleet of Print Devices deployed to support the GovPrint service |
| Follow Me Print / Pull Print | User submits a print job from their PC/Laptop and goes to any Print Device to authenticate and release print jobs |
| GovPrint | Overall shared print service |
| GovPrint Cloud / the Service | Current tender for a GovPrint service |
| GovPrint2 | The second contract for a GovPrint service which is currently live and will expire in 2029 |
| Hub / Authority Hub | Multi occupancy building managed by Authority |
| MFD / Device / Print Device | Multi-functional device - device supporting print, copy and scan |
| Non Authority Locations | Locations managed by other government departments or agencies |
| OS / Operating Systems |  |
| SaaS | Software as a Service |
| SC | Security Check |
| Shared Print Service / GovPrint | The GovPrint service |
| SIAM | Service Integration and Management |
| SOW | Statement of Work to define and agree development work packages |
| Supplier / Suppliers / Print Service Supplier | Suppliers that provide components of the GovPrint service |
| VDI | Virtual Desktop Infrastructure |

# SCOPE OF REQUIREMENT

Key to the success of the GovPrint Cloud service will be the ability to meet a wide range of requirements from government organisations using the service either within Authority locations or clients own locations. It will also be important to standardise wherever possible to ensure a cost effective and efficient service.

The Authority also recognises that requirements will change over time. One of the main benefits of a SaaS delivery model is the ability to add new features and functions to the service. A programme of continuous improvement will be critical and the GovPrint Cloud service provider must continue to develop the service throughout the term of the contract. The Authority and the Supplier will work together to define requirements for new features and functions and agree on a product development road map.

As outlined previously this tender is for a single supplier to provide the GovPrint Cloud service. The service must support content that is classified as OFFICIAL. The supplier will provide the following components:

* Cloud Print Service - Cloud SaaS providing printing and scanning services
* Deployment Services - service standup, location on-boarding and client on-boarding
* Operational Services - support, maintenance, service operations, service delivery management and contract management

To deliver operational services the supplier will need to work with a number of other organisations and suppliers to deliver efficient services. This will include device suppliers i.e. suppliers on RM6361 and RM6174, client service desks, Authority ITSM service providers and FM service providers.

The contract must support the ability to roll out and deliver the service to Authority and non Authority locations.

The Authority wants interoperability between the GovPrint Cloud service and the service provided as part of the current GovPrint service provided by Xerox UK Ltd / Cirros Document Solutions Ltd.

# THE REQUIREMENT

## Commercial Requirements

The GovPrint Cloud service will be procured via a two stage Restricted Procedure Competition. The contract is for an initial term of 3 years and six extension options of 1 year each (3+1+1+1+1+1+1), for a maximum contract length of 9 years.

### General Commercial Requirements

The Authority requires the GovPrint Cloud service to offer flexibility and the commercial structure must support the following:

* Ability to roll out the service to Authority and non Authority locations
* The Supplier must not impose any minimum volume commitments, for example minimum number of users or devices, attached to Authority as a whole or to individual devices or services
* The Supplier will be required to work with hardware suppliers selected for the CCS RM6361 Lot 4 GovPrint and allow these suppliers to connect compatible devices to the GovPrint Cloud service. The Authority requires the Supplier to continue to expand the range of supported devices throughout the term of the contract.
* Authority will require service credits linked to defined SLA performance measures
* The supplier must agree to support the following service contract structure:
  + Authority will have a contract with the Supplier with a master agreement for full service with Supplier
  + Authority will have a Memorandum of Understanding (MOU) with each client using the service.
  + Call Off orders will only be placed once clients have signed the MOU
* The terms and conditions of this contract will apply to any purchase orders placed
* The Supplier will be responsible for ensuring that they have the rights to deploy and operate all software solutions provided to the Authority as part of the contract and for the full period of the contract
* The Supplier must ensure that they have the correct licensing and suitable support agreements in place to deploy, maintain and operate all products including hardware and software solutions provided to Authority as part of the contract and for the full period of the contract
* TUPE – Authority considers that TUPE regulations do not apply to any contracts awarded or call off orders placed under this agreement

## Technical Environment

All components of the proposed solution must fully support the IT infrastructure deployed to support the Authority Hubs and support typical client IT infrastructure environments.

### Authority IT Infrastructure

The following IT Services will be provided in an Authority Hub.

**Shared Network**

Authority provides a shared network in Authority hubs with the following key capabilities:

* Cat 6 fixed cable with 1GB Ethernet with 802.1x access control using X.509 certificates
* WiFi 802.11ac
* GovWifi - preferred connection method with 802.1x access control, note that GovWifi deploys client isolation and supports Internet only external connectivity with outbound initiated connections
* Building Wifi - 802.1x access control, devices allocated to Print VLAN (see below description of Print VLAN)
* IPv4
* Support for 802.1x authentication
* Fixed network cable using X.509 certificates
* Building Wifi and GovWifi use WPA2-Enterprise supporting authentication using EAP-PEAP and EAP-TLS. EAP-TLS is the preferred method using CA issued X.509 certificates.
* DHCP, DNS and NTP services
* The Authority Shared Network will provide a Print VLAN supporting the following:
* Communication between devices located within the Print VLAN only (no communication between the Print VLAN and other VLANs in the hub or to any devices connected via GovWifi)
* Internet only external connectivity with outbound initiated connections
* No support for inbound initiated connections, VPN connections or NAT support
* Devices will be allocated to the Print VLAN using Certificate Authority (CA) issued X.509 certificates (device certificates will be issued and managed by the print hardware supplier)
* Devices connected via fixed connections or Building Wifi can be allocated to the Print VLAN
* Devices can be connected via Cat 6 cable or Building Wifi
* All Print Devices required to deliver the GovPrint service within the hub will be allocated to the Print VLAN
* Devices connected to GovWifi cannot be allocated to the Print VLAN and will only have direct access to the internet. There will be limited restrictions on the ports or protocols supported and most IANA defined ports should be supported.
* There is no Wide Area Network (WAN) connectivity between each Authority Hub or location
* Internet connectivity
* Internet connectivity via agreed ports / protocols / URLs
* No support for VPN connection to or from a building / location to the cloud service
* No support for in-bound initiated connections
* No support for in-bound firewall rules
* No support for Network Address Translation (NAT) or public facing IP addresses
* On-premise infrastructure:
* There is no capacity for any on premise infrastructure to support the GovPrint Cloud service including connecting print devices to the GovPrint Cloud
* The requirement is that the only on-premise infrastructure required will be the print devices and that these devices can connect to the required cloud services directly with no need for on-premise servers, appliances or other hardware
* There are no infrastructure resources e.g. servers, available on site or in the cloud to host any software or agents required to support the service

### Client IT Infrastructure

**End User Compute**

Where components are deployed in the client’s end user compute environment they must fully support the typical IT infrastructure deployed by clients using the service, this will include the following:

* Clients will provide their own department End User Compute (EUC) devices e.g. laptops, desktops and mobile devices
* Department EUC device Operating Systems (OS) to be supported will include:
* Microsoft Windows
* Apple Mac OS
* Chromebooks
* Mobile clients – iOS and Android
* Client EUC devices connected to the Hub Shared Network will not have access to other resources on the shared network such as Print Devices located on the Print VLAN
* Some clients may provide EUC services via Virtual Desktop Infrastructure (VDI)
* Some clients may provide print services via host based systems

**Network Infrastructure**

Where print devices are deployed within client IT environments i.e. in non Authority hub locations, they will typically be deployed in the following environment:

* Cat 5 / Cat 6 fixed cable with 1GB Ethernet
* 802.1x access control using X.509 certificates or MAC Address Bypass (MAB)
* WiFi 802.11ac with WPA2-Enterprise (X.509 certificates or username / password) access control or WPA2-PSK
* GovWifi (with client isolation enabled)
* IPv4
* IPv6
* DHCP, DNS and NTP network services
* Internet connectivity
* Internet connectivity via agreed ports / protocols / URLs
* No support for VPN connection to or from a building / location to the cloud service
* No support for in-bound initiated connections
* No support for in-bound firewall rules
* No support for Network Address Translation (NAT) or public facing IP addresses
* On-premise infrastructure:
* There is no capacity for any on premise infrastructure to support the GovPrint Cloud service including connecting print devices to the GovPrint cloud
* The requirement is that the only on-premise infrastructure required will be the print devices and that these devices can connect to the required cloud services directly with no need for on-premise servers, appliances or other hardware
* There are no infrastructure resources e.g. servers, available on site or in the cloud to host any software or agents required to support the service

Devices connected to GovWifi will only have direct access to the internet. There will be limited restrictions on the ports or protocols supported and most IANA defined ports should be supported.

The range of ports used should be limited and the solution should adopt IANA defined ports wherever possible.

There are no internal communication routes between EUC devices and Print Devices.

## Service Delivery

### Authority Hub Service Delivery

The full end to end print service will be provided in Authority hubs via four service providers:

* GovPrint Cloud service provider - the services provided by the Supplier selected based on the outcome of the competition
* Print Device (hardware) service provider - provision and support for print devices
* Hub IT Service Management Service Provider (ITSM Service Provider) delivering the following services:
* Service Desk
* Hub onboarding support
* Network operations and management
* Client service desk (the service desk operated by clients using the GovPrint service)

The GovPrint Cloud service supplier must work with all parties to ensure efficient operation of the service.

### Non Authority Hub Service Delivery

In non-Authority Hubs the detailed service model will vary. The detailed service delivery model will be defined on a case by case basis but the range of services provided by the Supplier will remain the same.

### Building / User Identity Pass

The GovPrint Cloud service including print devices and the Cloud Print Service must support a wide range of commonly used building / user identity pass standards.

Where possible the Authority will be standardising on GovPass cards.

The service must support the following:

* Card Reader
  + Print device suppliers will provide a multiformat card reader capable of:
    - reading the Static Serial Number from a wide range of commonly used proximity cards
    - reading the encrypted Print App on GovPass cards - further details can be found in Appendix A - GovPass
* GovPass Cloud User Authentication
  + Support the use of the Static Card Serial Number for user authentication
  + Support the use of the serial number included in the secure Print App on GovPass cards for user authentication

### GovPass Card Validation

The Authority wishes to implement GovPass card validation within the Cloud Print Service. To support this the Cloud Print Service must be able to make an API call to the GovPass service to confirm the GovPass card is valid before allowing an authenticated user to access the service. The Authority wishes to implement this functionality within 6 months of the service going live. Further details of the GovPass API are included in Appendix A - GovPass.

For the avoidance of doubt, in locations where GovPass cards are not used there will be no requirement to confirm the validity of the card.

The costs for development of this capability must be included in the Suppliers proposed costs in Attachment 4 of the ITT pack Price Schedule.

## Cloud Services

### General Approach

The Supplier must deliver the GovPrint Cloud service via a multi-tenant Software as a Service (SaaS) service model and a public cloud deployment model.

The Supplier must provide the GovPrint Cloud service via a fully cloud based service with no on premise hardware or software components (with the exception of any required client software deployed to EUC client devices or installed on Print Devices).

### Print Devices

The GovPrint Cloud service must be compatible with a wide range of print devices including multi-functional devices (MFDs) and single function printers from leading print hardware manufacturers.

The Supplier will be required to maintain a list of fully compliant print devices that can be connected to the Cloud service. The Authority will ensure that only devices on this list will be connected to the service.

Compliant print devices will be procured via a range of sources including relevant CCS frameworks.

The Authority intends to procure devices via the CCS RM6361 Lot 4 GovPrint and future iterations of the CCS MFD frameworks.

Key requirements for a hardware supplier to be awarded a place on CCS RM6361 Lot 4 GovPrint include:

* The ability to provide a catalogue of print devices that are fully compatible with the GovPrint Cloud
* All print devices will be fully tested to ensure they are compatible with the GovPrint Cloud
* Actively work with the GovPrint Cloud support including testing of device compatibility and resolution of any incidents

The Authority wishes to connect a wide range of devices to the GovPrint Cloud service. In addition to the devices available via CCS RM6361 Lot 4, The Authority wishes to expand the range of devices supported to include a wide range of compatible devices such as label printers, wide format and high volume devices. The proposed solution must offer scope to extend the range of devices beyond the devices available via CCS RM6361 Lot 4.

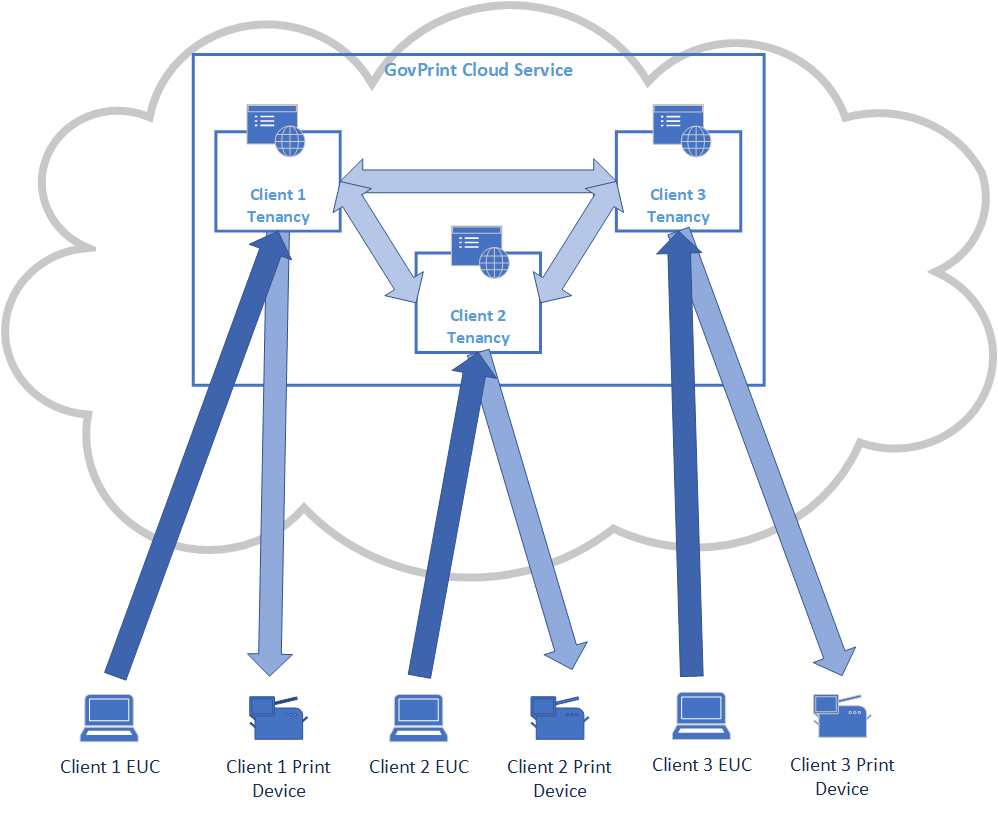
### Cloud Print Service Delivery Model

The Supplier must provide a fully cloud based solution to support a print, copy and scan service.

The proposed solution must support the following capability:

* Multi-tenant Software as a Service (SaaS) service model and a public cloud deployment model
* As the service scales the aggregation of data across government via a single service such as the GovPrint Cloud presents an increasing security risk, the Authority may wish to adopt the following evolution for service delivery and the proposed solution must be able to support this approach
  + Public Cloud shared instance
  + Public Cloud dedicated instance
  + Private Cloud dedicated instance
* The supplier must ensure that adequate controls are in place to mitigate the risks of data aggregation. This will include applying appropriate separation of data between clients. NCSC Cloud Security Principle 3 will be applicable to this requirement.
* Logical Tenancy Structure
* Support a logical tenancy structure as outlined in Diagram 1 that enables
  + Each client to have their own tenancy within the GovPrint Cloud Service
  + Each client’s EUC devices connect and submit print jobs to their specific tenancy
  + Each Print Device to be connected to a tenancy and shared across all tenancies within the GovPrint Cloud service
  + Users submit print jobs to their Client Tenancy but can release print jobs on any Print Device

Diagram 1 - High Level Logical Tenancy Structure



* Network Support
* Support network infrastructure as outlined in section 6.2.1 Authority IT Infrastructure
* Support network infrastructure as outlined in section 6.2.2 Client IT Infrastructure
* Critical requirements include but are not limited to:
  + Secure (TLS) outbound connections only, no requirement for inbound connectivity, VPNs, NAT or similar
  + No requirement for direct connectivity between EUC devices and Print Devices, all communication via the GovPrint Cloud
  + No requirement for any on-premise hardware or software other than client software installed on EUC devices and print devices
* User Authentication and Access Control
* Support a wide range of user authentication solutions / services including but not limited to:
  + Cloud - MS Entra ID (Azure AD), OpenID Connect, Google, Okta, PING
  + On Premise - LDAP, Active Directory
* Each client accessing the service will have their own independent identity management solution / service that will be managed by the client
* There will not be a central identity source that can be used by the service to support user authentication and the service must be able to integrate with multiple independent identity services
* Each client tenancy can be linked to the client’s identity management solution
* Tenancy Functionality
* The ability to set key settings at a tenancy level e.g. job TTL, print job defaults e.g. mono / colour, simplex / duplex, scan to email max file size / default file type etc
* Tenancy management via Service Dashboard

### GovPrint Cloud Clients

The GovPrint Cloud must provide the following components.

**End User Compute (EUC) Client Software**

Any EUC Client software required to be installed on EUC devices must provide the following:

* Support the following EUC operating systems
* Windows – Win 10 / Win 11 (32 and 64bit) plus any future updates and releases
* Mac OS 10 plus any future updates and releases
* Enable a single client supporting:
* multiple manufacturers print devices with a specific emphasis on the manufacturers products available via RM6361
* Support as a minimum the selection of:
  + Pages
  + Copies
  + N-up
  + Mono / colour
  + Simple / duplex
  + Paper size and orientation to be defined by the document being printed with override within the EUC client
  + Support non standard paper sizes e.g. FP10 prescriptions
  + Paper source
  + Paper type
  + Finishing options - staple, sort and punch
* Provide user with job costs estimate prior to job submission
* Be digitally signed
* Must be updated as required to support releases of updated EUC device OS as they are released by the OS vendor
* Must support the ability to be packaged and deployed via automated process such as Group Policy or deployment tools such as MECM, this must include delivery of updates
* After initial deployment, support updates to EUC Client managed from the cloud service (subject to any EUC device / OS limitations or controls). This must include the ability to update tenancies and UEC Clients within tenancies independently.
* Support client endpoint authentication using X.509 certificates using Certificate Authority (CA) issued certificates
* The cloud service must only accept incoming connections from authenticated and trusted endpoints

**Print Device Client Software**

Print Device client software to be installed on each Print Device must support:

* User authentication and access control
* Support print, copy and scan services without the need to access Print Device native functions
* Control access to Print Device native functions
* Certified by Print Device vendor if the Print Device vendor offers a certification program
* Be digitally signed
* Available for multiple manufacturers Print Devices including products from all manufacturers who have products available via CCS frameworks
* Provide a consistent look and feel across all supported Print Devices
* Provide intuitive workflows to support registration, user authentication, follow me print, scanning and copying
* Where applicable support Web Content Accessibility Guidelines (WCAG) 2.2 or other accessibility guidance
* Support remote deployment and updates from the GovPrint Cloud or the relevant manufacturers cloud device management solution
* The cloud service must only accept incoming connections from authenticated and trusted endpoints
* Support client endpoint authentication using X.509 certificates using Certificate Authority (CA) issued certificates

**Service Dashboard**

* The GovPrint Cloud service must provide a service dashboard
* The dashboard must support Role Based Access Control (RBAC)
* Roles will include but are not limited to; admin, support and user and access to functionality provided by the portal will be restricted based on role
* The portal will enable The Authority and clients to:
* Monitor the GovPrint Cloud Service
* Client admins and support to manage their tenancy including:
  + - Setting tenancy defaults
    - Manager users e.g. remove linked cards
    - Access reporting
    - Manage delegate printing
    - Manage release all printing
    - Manage direct / push printing
    - Manage print room / job ticketing
* Client users to manage their account including send / resend password and review print volumes
* The portal will provide a subscription service for service updates. This service will be used to inform clients of service updates. Clients will be able to subscribe to updates and will receive updates via their registered email address. The subscription service will include details of all planned changes and current service performance issues.

### GovPrint Cloud Service Functionality

The GovPrint Cloud Service must support the following functionality.

**Pull Print / Follow Me Print**

* Provide a Pull Print / Follow Me Print service i.e. users submit a print job(s) to the service and then goes to any Print Device connected to any tenancy within the GovPrint Cloud to authenticate and release their print job(s)
* Single Print queue regardless of location or target device
* Print Job Submission
* Submission must be supported via:
  + - EUC Device Client using ‘file>print’ functionality
    - Upload to web portal / dashboard
    - Email with print job attachment
* Default print settings can be set including duplex and mono output at a tenancy level. Users can select to change these for each job/application session.
* Support secure transfer of the print job to the GovPrint Cloud service
* Performance requirements
  + - If a window or pop up is required to submit a print job to the cloud service this must be displayed within 5 seconds of the user requesting to submit a print job e.g. by clicking the ‘print’ button
    - Submission of print jobs to the cloud must be completed in an acceptable timescale, for example submission of a 10 page print job must not take longer than 5 seconds after the user clicks the relevant ‘print’ button to begin submission of the print job to the cloud service.
    - Where submission of print jobs will take longer than 5 seconds e.g. for documents over 10 pages, print job submission must be completed in the ‘background’ allowing the user to continue to work while the job spools.
* Print Job Release
* Print job release must be completed via the Print Device Client installed on the print device
* Print Release Workflow at Print Device
  + - User authenticates at the Print Device using a range of RFID cards including GovPass
    - User can authenticate with username and password / PIN code as secondary logon method
    - User can review list of submitted print jobs
    - User can select single, multiple or all jobs
    - User can select action: Print, Print & Save or Delete
    - User can select to modify key job attributes at the Print Device e.g. number of copies, colour / mono, simplex / duplex etc.
    - User can select additional options available at the releasing Print Device e.g. select stapling, sorting etc
    - Non-collected print jobs deleted after the tenancy job TTL value
    - Performance requirements
    - User authentication at the MFD using a registered card must take no longer than 3 seconds i.e. within 3 seconds of the user placing their card on the card reader the main menu for the cloud print service will be displayed on the control panel of the print device
    - Print jobs must start printing within 5 seconds of the user selecting ‘print’ on the print device (for the avoidance of doubt ‘start printing’ is defined as the point where the print device starts to process the print job)
* Delegate Printing
  + - User can delegate release of their print job to another user
    - This capability can set at the user level
    - Configuration of delegate printing will be available to admins via the Dashboard
* Release All
  + - User can be configured to have all stored print jobs released once they have authenticated e.g. user authenticates at a Print Device with their card and all stored print jobs for the user are released at the device
    - This capability can be set at the user level
    - Configuration of delegate printing will be available to admins via the Dashboard

**Direct Print**

* Provide a Direct Print service i.e. users submit a print job to be printed on a specific device, once the job is submitted it is printed immediately on the specified device
* Direct Print must not be limited to devices in the local building and must not require local connectivity between the EUC device and Print Device i.e. direct print jobs must be routed via the GovPrint Cloud
* Manage access to Direct Print functionality via the Service Dashboard:
* Client Admins can control which devices are available for push print / direct print within their tenancy
* Client Admins can control which users can print to available push print / direct print Print Devices and which devices they can print to
* Performance Requirements
* If a window or pop up is required to submit a print job to the cloud service this must be displayed within 5 seconds of the user requesting to submit a print job e.g. by clicking the ‘print’ button
* Submission of print jobs to the cloud must be completed in an acceptable timescale, for example submission of a 10 page print job must not take longer than 5 seconds after the user clicks the relevant ‘print’ button to begin submission of the print job to the cloud service.
* Where submission of print jobs will take longer than 5 seconds e.g. for documents over 10 pages, print job submission must be completed in the ‘background’ allowing the user to continue to work while the job spools.
* Print jobs must start printing within 5 seconds of completing print job submission to the cloud (for the avoidance of doubt ‘start printing’ is defined as the point where the print device starts to process the print job)

**Print Room / Offsite Print Service Job Submission**

* Support job submission to Print Room or Offsite Print services via email with PDF format job and Job Ticket
* Support job submission to Print Room or Offsite Print services via RESTful API call with PDF format job and Job Ticket
* Job ticket contents to be customisable and defined at a tenancy level

**Print Rules**

* Ability to implement print rules to manage user behaviour such as:
* Enforce double sided printing
* Enforce mono printing
* Enforce print quotas
* Route jobs to Print Room or specific Print Devices
* Rules to be defined and implemented at a tenancy level

**Scanning**

* Scan to Email
* Default destination is users registered email address
* The sent from address must be defined in each tenancy
* Support multiple delivery methods including:
  + Scan job attached to email
  + Secure download link for scan job attached to email
  + Smart routing based on file size i.e. scanned documents below a specific size routed as attachments and files above a specific size routed as secure links (attachment size can be set at a tenancy level)
* Scan to cloud destinations
* Support a range of common cloud storage services including but not limited to Microsoft OneDrive, Google Drive, Dropbox etc.
* Scan to clients specific tenancy within their cloud storage service
* Default settings can be set at a tenancy level
* Scan Settings
* Support the ability to set a range of Scan Settings at tenancy level including resolution, file format, file name, mono/greyscale/colour etc.
* User can change default settings at Print Device when they scan a document
* File Formats
* The solution must support output of files in a range of formats including:
  + Searchable PDF/A
  + TIFF
  + JPG

**Payment Service**

In future The Authority may wish to support pay for print services.

* The service must be able to support pay for print services
* Support cashless payment for print jobs released

**User Authentication and Authorisation**

* Support loosely coupled integration with each clients identity and access management (IdAM) solution to support user authentication and access control
* Integration with the clients IdAM solution must not require the end users full credentials i.e. username and password to be shared with the GovPrint cloud
* User Registration workflow
  + User can either submit a print job or enter their email address on the Service Dashboard to begin registration
  + If the user is a member of GovPrint access group defined in the client’s IdAM service the registration process can continue
  + The user will receive via email a password that can be used to complete the registration process
  + If the user is removed from the GovPrint access group in the clients IdAM solution the user will also have their access to the GovPrint service revoked
* User ID / Building Card Registration
* Card self-registration process at Print Device using username/email address and password issued to user as part of User Registration

**Tracking, Auditing and Reporting**

* User Level Reporting
  + Track user level print, copy and scan activity across all print devices including recording user, device, date/time and job details e.g. file name etc. to support requirements defined in section 8 Management Information / Reporting
  + Within each tenancy client admins can access user level reporting across all Print Devices for users within their tenancy
  + The Authority can access user activity reporting aggregated at a tenancy level i.e. The Authority does not have access to user level information but can access reports at a tenancy level
* Device Level Reporting
  + Track device level print, copy and scan activity across all print devices to support requirements defined in section 8 Management Information / Reporting
  + Within each tenancy client admins can access device level reporting across all Print Devices within their tenancy
  + The Authority can access device level activity across all devices across all tenancies

### Cloud Print Service Interoperability

The Authority has delivered the current GovPrint service to multiple hubs and client locations and is now looking for a supplier to deliver the GovPrint Cloud service.

The ability for users to access shared print services across all locations is a key requirement and interoperability between the GovPrint Cloud Service and the current GovPrint service is critical.

The current GovPrint service is delivered by Xerox using Cirros Document Solutions cloud print management.

The Authority recognises the potential complexity and difficulty in delivering this requirement and is willing to consider alternatives to having full interoperability available from day one of the GovPrint Cloud service.

The Authority expects interoperability to be delivered using API functions provided by the current Cirros cloud service and the Suppliers cloud service. Appendix B - Interoperability provides a summary of the expected API capabilities required to support interoperability between the cloud services.

In addition to delivering interoperability between the Supplier’s service and the current GovPrint service, The Authority wishes to move to a future service delivery model based on a GovPrint ecosystem delivered by interoperable print services (Cloud + Devices) from multiple manufacturers. The supplier will be required to actively support the development of interoperability between their solution and other suppliers solutions.

## Service Standup

### Service Design

The Authority will work with the selected Supplier to fully define and document the products and services to be delivered by the Supplier and Authority. This will include agreeing and documenting responsibilities for each party and the production of a comprehensive Service Design Document.

The Service Design Document will cover the following designs:

* The overall design of the service
* A standard design for each location / client as it onboards to the service

### Proof of Concept

The Supplier must implement a Model Office prior to the deployment of the production service. The Supplier will provide all infrastructure required to support the proposed solutions. Authority will provide the services outlined in Section 6.2.1 Authority Hub IT Infrastructure.

The Model Office will be used for the following:

* Demonstrating the service can meet the Authorities requirements
* Demonstrating the service to prospective Authority clients
* Reference environment to define device and software configuration prior to deployment
* Testing and evaluation
* On-going support

### Production Service Stand-up

The purpose of Service Stand-up is to deploy all infrastructure and services required to deliver the Service before onboarding the first location / hub. This will include but is not limited to:

* Overall Service Design
* Project Management
* Configuration of proposed cloud services
* Deployment of Model Office for testing and evaluation
* Stand Up of Operational Services
* Testing and evaluation

## Deployment Services

### Project Management

The Authority requires the deployment of the service to be actively managed by all parties including the Supplier, The Authority and all other suppliers engaged as part of the delivery of the service for any specific location or client.

The Supplier must assign a named Project Manager for each client onboarding to the service.

The Authority will appoint a named Delivery Manager to work with the Supplier.

The Supplier must work jointly with the client and any hardware suppliers deploying devices that will be connected to the cloud service.

The Supplier will follow Authority’s standard project approach which may include, but is not limited to:

* Structure & Governance
* Project Board
* Project Team
* Documentation
* Project Plan
* Work Packages & Deliverables
* Project Logs and Registers
* Project Reporting

The overall aim of Project Management will be to deliver the project on time, within budget and to agreed quality levels.

### Training

Training is critical to user adoption and overall success of the service.

The overall aim must be to minimise the need for end user training i.e. the service must be intuitive for end users and administrators to use.

The Supplier must offer a blended approach to training and will offer a range of methods for training including on-site, on-line and user documentation.

The Supplier must provide a range of training options aimed at different target audiences including but not limited to client end users, client admins, The Authority and ITSM Service Provider staff.

The Supplier must provide training for all elements of the proposed solution including hardware, software solutions and services.

The Supplier must work with Authority to create an agreed training package to support the deployment. The training package should include but is not limited to:

* Client on-boarding training and documentation
* Service Desk fault guide and triage for Client and ITSM Service Provider Service Desk

The Supplier must provide a suitable training service throughout the contract term.

Training and technical documentation for all elements of the service must be made available in electronic format e.g. searchable PDF and should include user guides, user posters, user manuals and admin manuals.

The Supplier must provide update training and documentation as reasonably required when new versions or products are released.

### Location On-boarding

The purpose of Location On-boarding is to deploy all infrastructure and services required to deliver the Service into one or more locations. This will include but is not limited to:

* Location Service Design
* Project Management of onboarding activities
* Configuration of proposed Cloud Print Service
* Support configuration of network infrastructure in the location / hub
* Support testing and evaluation

### Client On-boarding

The purpose of Client On-boarding is to efficiently deploy all infrastructure and services required to deliver the Service to meet a specific client's needs. This will include but is not limited to:

* Client Engagement
* Client IT Integration
* Testing and evaluation

*Client Engagement*

The Authority will be responsible for the initial engagement with clients that wish to consume the service. Once a client expresses an interest in the service, The Authority will pass the opportunity to the Supplier to fully manage the client onboarding process. The aim will be to have an efficient and effective process that can optimise the onboarding process, reducing time and cost for all parties. The Supplier must fully project manage the deployment of the service.

*Client IT Integration*

The aim of client IT integration is to ensure integration between the client’s IT infrastructure and the Cloud Print Service. This will include:

* Integration with the client’s identity service to support identity management
* Support for deploying any EUC Client software or drivers on EUC devices
* Integration with the clients cloud storage if the client is using a supported cloud storage platform

## Operational Services

### Service Desk

**Call Escalation**

Escalation of end user issues will follow the following workflow:

* End user experiencing an issue with the print service will log a call with their Departmental Service Desk
* The Departmental Service Desk will triage the call and escalate as follows:
* Escalate to the Supplier if the issue relates to the Print Service
* Escalate to the ITSM Service Provider for the hub / location if the issue relates to hub infrastructure e.g. the shared network
* If call escalated to the ITSM Service Provider are not related to the hub / location infrastructure the call will be returned to the Departmental Service Desk

**ITSM Service Provider Service Desk**

The ITSM Service Provider provides a range of IT support and management services within a hub including a Service Desk. The ITSM Service Provider will provide a Service Desk during ‘Business Hours’ as defined in Section 15 Service Level Agreements. The Departmental Service Desk will be able to log calls with the ITSM Service Provider Service Desk. The Service Desk will triage calls and those determined to be due to products, solutions or services provided by the Supplier will be escalated to the Supplier Service Desk via the following routes:

* Service Portal
* Email
* Telephone

Authority wishes to move towards improved integration between service desks and support call escalation via API / structured messages. The Price for this development will be agreed at a later date using the Suppliers SFIA rate.

The Supplier will work with Authority and the Hub ITSM Service Provider Service Desk to develop an agreed triage process.

**Supplier Service Desk**

The Supplier will provide a Service Desk service during ‘Core Operational Hours’ as defined in section 15 Service Levels and Performance.

The Supplier must be able to support escalation of calls via the following routes:

* Service Portal
* Email
* Telephone

Authority wishes to move towards improved integration between service desks and support call escalation via API / structured messages.

The Supplier Service Desk will review and triage the call. If the call is within scope of the services provided by the Supplier, the Supplier will resolve the issue and formally close the call. If the call is out of scope of the services provided by the Supplier the Supplier can reject the call returning it back to the service desk that escalated the call.

Calls / service requests deemed to be in scope for the Supplier are:

* Cloud Print Service faults and issues
* Fulfilment of authorised Change Requests

The Supplier must provide a Service Portal to allow the client Service Desk and ITSM Service Supplier Service Desk to track the following:

* Status of all open calls – including those raised by any device monitoring software deployed as part of the software solution
* Other relevant services provided by the Supplier as part of the contract e.g. change requests

The Authority and the Supplier will work together during Service Design to agree and fully document the Service Desk processes including a full escalation process.

**Supplier Service Desk Extended Support (optional)**

The Authority may require support for Extended Business Hours as defined in Section 15 Service Levels and Performance. The delivery of this service will be on a case by case basis based on the requirements of specific organisations.

The Service Level Agreement for this service including service hours and response times is documented in section 15 Service Levels and Performance.

### Cloud Service Management and Support

The Supplier will be responsible for the management and support of the GovPrint Cloud service.

The Supplier must resolve all reported software service faults as defined in section 15 Service Levels and Performance.

The Supplier must ensure that the software solutions meet the Service Level Agreements defined in section 15 Service Levels and Performance.

The Supplier must maintain all software at the latest version(s) recommended by the software supplier.

The Authority and the Supplier will agree a firmware / software update policy.

All updates will be managed via the agreed change management process.

Where updates to any EUC client software can be managed via the cloud service, the Supplier will be responsible for applying updates.

The Supplier must inform The Authority and clients using the service via the subscription service of all updates prior to delivery / installation of the update within the following timescales:

* Cloud Service - 1 week
* Cloud Service Print Device Client - 2 weeks
* Cloud Service EUC Client - 2 weeks

Any software updates required to mitigate identified security issues must be applied as soon as is practicable.

The Service Level Agreement for this service is documented in section 15 Service Levels and Performance.

### Change Management

**Change Requests**

All Change Requests for software changes will be raised via the Authority Change Management process.

The Change Request process will include a fortnightly Change Board where all changes will be reviewed and actions agreed.

# KEY MILESTONES AND DELIVERABLES

Table 5 - Key milestones and deliverables

| Milestone/Deliverable | Description | Timeframe or Delivery Date |
| --- | --- | --- |
| 1 | Initial Service Design (technical and services high level design) | Nov 2024 |
| 2 | Proof of Concept Build and Testing | Jan 2025 |
| 3 | Production Service Design | Feb 2025 |
| 4 | Production Service Standup Complete | Feb 2025 |
| 5 | Test and Remediation | Mar 2025 |
| 6 | IT Health Check / Remediation | April 2025 |
| 7 | Operational Services Standup | Mar 2025 |
| 8 | Service Documentation | April 2025 |
| 9 | Production Service Live (ready to start client onboarding) | May 2025 |
| 10 | Interoperability Discovery | Jan 2025 |
| 11 | Interoperability Design | Feb 2025 |
| 12 | Interoperability Build | May 2025 |
| 13 | Interoperability Testing | Jun 2025 |
| 14 | Interoperability transition to Live Service | Aug 2025 |

# MANAGEMENT INFORMATION/REPORTING

### 

The detailed structure and content for Management Information (MI) will be agreed during Service Design.

## Management Information

The Authority requires the following core information to be available.

* Data available daily / current i.e. live activity reporting
* Device level print, copy and scan volumes
* User level print, copy and scan volumes
* Job details including recording user, device, date/time and job details including but not limited to file name, file size, pages and copies, function (print, copy, scan) etc.
* Data available monthly / management information
* Billing data
* Device activity and utilisation
* SLA reporting
* Cloud service performance including:
  + - Availability
    - Capacity
    - Benefits realisation - to be agreed during the initial contract term.
    - Environmental impact / sustainability reporting - to be agreed during the initial contract term.

As outlined previously the Authority will not have access to user level information held within each client’s tenancy. To summarise this:

The Authority have access to:

* Department level volumes
* Device level volumes

Clients have access to:

* User level volumes
* Individual job details
* Device level volumes

The MI requirements will change over the period of the contract and therefore the Supplier must offer flexibility to allow MI to be adapted as required throughout the length of the contract.

## Access to Reports

Access to MI must be via the Suppliers Service Dashboard which will be available to The Authority and Client Administrators. Client Administrators must only have access to information that is for their specific organisation e.g. reporting for their specific tenancy within the service.

The Service Dashboard must provide the following:

* Access to all core information
* Range of standard reports
* Ability to create custom reports
* Ability to schedule standard reports

The Supplier must submit all required reports to support Service Delivery Management in electronic format e.g.

* Text based reports via PDF
* Data based reports via Excel / CSV

The Authority is developing a Reporting Portal and will require the supplier to support importing of GovPrint Cloud reporting data into the Authority Reporting System. Methods for importing data may include:

* Data importing using CSV files
* Data importing via API (full specification to be defined)

The supplier must be willing to work with the Authority to implement this.

# VOLUMES

## As outlined previously the specific number of devices will be dependent on a range of factors including:

## The number of Authority locations the service is rolled out to

## The number of clients that subscribe to the service in each Authority location

## The number of client users

## The number of non Authority locations the service is rolled out to

The Authority has used the following parameters to model an indicative number of devices over the term of the contract:

* Planned Authority hubs
* Estimated adoption of service from clients occupying each Authority hub
* Estimated adoption of service for non Authority locations
* Estimated number of users

Table 6 provides a summary of the output from the model including the indicative number of deployed Print Devices across Authority and non Authority locations. . The indicative volumes will be used to calculate a Total Cost of Ownership (TCO) for the service based on the pricing information provided by the supplier. This TCO calculation will be used to evaluate the price element of the supplier's bid.

These figures are indicative and Authority does not guarantee the number of devices to be deployed.

Table 6 - Indicative Print Devices across Authority and non Authority locations

| **Year** | **Deployed Print Devices** | **Fleet Size** |
| --- | --- | --- |
| 1 | 500 | 500 |
| 2 | 1,500 | 2,000 |
| 3 | 4,000 | 6,000 |
| 4 | 5,000 | 11,000 |
| 5 | 6,300 | 17,300 |
| 6 | 8,000 | 25,300 |
| 7 | 9,000 | 34,300 |
| 8 | 9,000 | 43,300 |
| 9 | 10,000 | 53,300 |

As detailed within this SOR there will be a limited requirement for development of the suppliers solution within the contract term to support interoperability and other critical objectives of GovPrint. To manage expectation the Authority anticipates the total amount of development within the full contract term to total £500,000, however this is indicative and subject to the development need for the GovPrint Cloud service as the service is deployed widely across the government estate.

# CONTINUOUS SERVICE IMPROVEMENT PROGRAM

The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

The Supplier must present new ways of working or functionality to The Authority at the Change Control Board meetings.

The Authority will present new requirements to the Supplier at the Change Control Board meetings. The Authority and Supplier will review requests and agree whether the requirements can be added to the product development road map. The Authority and the Supplier will work together to agree any associated costs for agreed changes.

The continuous service improvement program (CSIP) is intended to review service performance from previous ticket, monitoring, feedback and other data in order to further improve and refine the service. Improvements will typically include but not be limited to greater service availability and/or capacity, better user experience, reduced costs, meeting new or emerging requirements and/or refined service performance criteria. The authority accepts that some CSIP actions may require formal contract change.

Changes to the way in which the Services are to be delivered must be brought to Authority’s attention and agreed prior to any changes being implemented.

The Supplier must work with all vendors on the relevant CCS frameworks to ensure support for a wide range of devices from suppliers on the frameworks. This will include working with hardware vendors when new models are released.

# SUSTAINABILITY

## Sustainability

The Authority wishes to minimise the environmental impact of the GovPrint service throughout the period of the contract. This will include but is not limited to:

* Data centres hosting cloud services should comply with the EU Code of Conduct for Energy Efficient Data Centres
* Minimise the number of devices required to meet client print volumes
* Reducing the environmental impact of support services
* The Supplier will actively participate in the Authority’s programmes to reduce the environmental impact of hub buildings including:
* Continually review and provide feedback to the Customer on all relevant UK and EU legislation, policies, guidance and technology changes (including new product announcements) relating to sustainability
* Prepare within 180 days of Service Commencement Date and update at least annually, a consolidated road map and action plan demonstrating how they and the Other Suppliers will:
  + achieve business rules 1-3 of the UK Greening government: ICT and digital services strategy (2020-2025 or successor)
  + support the Customer to achieve the targets in the Sustainable ICT and digital services strategy: targets for 2020-2025 (or successor)
* Work with the Other Suppliers to reduce the overall carbon footprint baseline of the Services in line with the agreed target and timeline

The Supplier will be required to provide Authority every six months with consolidated sustainability information for the full service. This report will be aligned to support the production of central government STAR (Sustainable Technology Annual Report) returns that the Customer must submit under its Greening Government commitments and other reporting obligations and shall include. The full details of the reporting requirements will be agreed between Authority and the Supplier during the design phase.

## Social Value

## 11.2.1 Introduction

* The Authority takes its responsibilities to the communities it serves seriously, and in accordance with the Social Value Act 2012, it considers social value in all our decisions.
* Social Value (SV) refers to the wider financial and non-financial impacts of projects and programmes including the wellbeing of individuals and communities, social capital, and the environment.
* It is distinct from the deliverables of a contract and is the additional value that can be created for local communities or the wider public. By law, it must be considered throughout the commissioning cycle for goods, services or works by public authorities.
* This procurement will be run in accordance with the Public Services (Social Value) Act 2012 and PPN 06/20. As part of the tender process, Bidders will therefore be required to submit a social value proposal, which will account for at least 10% of their final overall bid evaluation score. This social value proposal will outline how Bidders intend to incorporate social value into their delivery of the required works.

## 11.2.2 The Social Value Model:

The Social Value Model (SVM) has been developed by the UK Government to provide a standard and proportionate way for commercial practitioners at all levels within central government departments, executive agencies, and non-departmental public bodies to identify, prioritise, evaluate, measure and report for Social Value in all stages of the procurement lifecycle. The focus during the tendering stage of a contract is on a qualitative assessment of Social Value, to encourage innovation, a diverse supply chain and a level playing field between bidders of different sizes and types. All organisations listed as being “in the scope” of [PPN 06/20](https://www.gov.uk/government/publications/procurement-policy-note-0620-taking-account-of-social-value-in-the-award-of-central-government-contracts) must use the SVM.

The SVM is designed to elicit high quality Social Value responses during the tender process from bidders. The successful bidder’s response will then form the basis of SV delivery during the contract phase. As part of the contract award process, the intention is to use the bidder’s tender proposals as the basis for setting Key Performance Indicators (‘KPIs’), which will be integrated into the contract management process. These KPIs will be mapped within the Social Value Portal to the Social Value TOM (Themes, Outcomes and Measures) SystemTM, designed for tracking and measuring all social value being delivered.

As part of its SV proposals, the Bidder must commit to regular reporting of social value delivery during the life of the contract using the Social Value Portal and the Social Value TOM SystemTM.

To facilitate effective delivery of the SV strategies proposed by bidders during the tendering stage, a mechanism is required to enable measurable targets to be set for monitoring during the contract management stage.

The KPIs will be agreed between the Authority and the Bidder following contract award using the Social Value TOM SystemTM to report on delivery and provide a proxy quantitative metric of SV generated. The Bidder will then develop and maintain a plan using these KPIs throughout the life of the commercial agreement, detailing how it will report on delivery of our SV priorities. It is of the utmost importance that reporting SV is accurate and uptodate and reflects the ambitions we agree upon.

## 11.2.3 Social Value TOM System™:

The Social Value TOM SystemTM is a proven social value mechanism that has been in use in public procurement since 2016 as a response to the requirements of the Social Value Act and it provides the delivery mechanism.

It is a transparent, open-source SV measurement framework which ensures compatibility and comparability in SV measurement. It provides robust and established measures endorsed by the National Social Value Task Force that connect with and map onto the reporting metrics provided in the SVM and the United Nations Sustainable Development Goals (UN SDGs).

Given the nature of this contract and the tender mechanism, we have not been prescriptive about the KPIs we expect for this contract and encourage bidders in the questions to make suggestions as part of their submission. These will be considered when agreeing KPIs with the successful bidder.

As part of their tender submission, bidders are requested to confirm acceptance in principle of the Social Value TOM system metrics as KPIs for the contract and / or comment as appropriate. This is a long-list of potential KPIs – the selection post contract award will depend in part on the successful bidder’s SV proposal.

Further information about the Social Value TOM SystemTM can be found [here](https://socialvalueportal.com/national-toms/).

Further information on the KPIs applicable to the MACs selected, and which will be agreed with the Bidder following contract award can be found in Appendix E.

## 11.2.4 Themes and Model Award Criteria (MAC)

* The Themes and Model Award Criteria (MAC) selected from the [Social Value Model](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940828/Social-Value-Model-Quick-Reference-Table-Edn-1.1-3-Dec-20.pdf) for this procurement are: [ 3. Fighting Climate Change, 4. Equal Opportunity and 5. Wellbeing ]
* The following MAC sub-criteria will be used:

| **Theme number and description** | **Model Award Criteria and sub-criteria description** |
| --- | --- |
| *3. Fighting Climate Change* | *4.1 Additional Environmental Benefits* |
|
| *4. Equal Opportunity* | *6.1 Tackle Inequality in the Contract Workforce* |
| *6.2 Supporting In-work Progression* |
| *5. Wellbeing* | *7.1 Support Health and Wellbeing in the Workforce* |

## 11.2.5 Working with SVP

The successful Bidder will be required to contract directly with the Authority’s Social Value partner who will provide the following services to the Bidder:

* Provision of an online account on the portal to enable contract management and project reporting in respect of SV;
* Technical support with data entry (e.g. access and functionality issues);
* Confirmation of evidence required to satisfy SV requirements and SV KPI targets;
* Provision of quarterly reports showing progress against SV KPI targets;
* Provision of an end-of-project summary report.

The successful Bidder will be invoiced directly by the Authority’s Social Value partner and will be responsible under the terms of the services contract for payment directly to the Authority's Social Value provider. By participating in the tender process, the Bidder confirms their unequivocal agreement with the Authority’s Social Value Partner’s [terms and conditions](https://socialvalueportal.com/terms-and-conditions/), and payment of the appropriate fees as outlined here:

## 11.2.6 Social Value Management Fee

There is no charge for Tenderers to access the Social Value Portal for the purpose of reviewing KPI’s in response to this tender.

For the successful Bidder awarded the contract only, there is a charge levied, (the "Social Value Management Fee"), to that Bidder to use the SV platform. This will help all parties track and manage SV delivery. The level of the Social Value Management Fee depends on the total value of the Contract. This is calculated as 0.15% of the total contract value (excluding VAT) per year, with a minimum fee of £750 per annum and a maximum capped fee of £7,500 (excluding VAT). If more than one Bidder is awarded a contract following a procurement, then each Bidder is liable for the amount as laid out in this document as SV benefits and reporting are individual to that bidder and project.

The fee will be charged quarterly in arrears by direct debit from the point at which the successful Bidder starts to deliver the services of the contract. This will be after the mobilisation phase of the contract and communicated to SVP by the Contract Manager of the contract. It is at this point that the Bidder will be granted access to, trained and login enabled to the **Social Value Portal**. Here the Bidder will record the social value that is delivered throughout the life of the contract.

For any contract that runs without a full final year, the Bidder will be charged on a pro-rata basis for each month of that contract’s final year up to 6 months. The Bidder will be charged for the full year if the contract end date is 6 months into the final year. These will still be paid quarterly, in arrears by direct debit.

**Example A: 17 Months - £3M**

A Contract is £3M, and therefore the annual fee would be £4,500 + VAT to use SVP, paid quarterly in arrears by direct debit after the point at which the Bidder starts delivering social value at a rate of £1,125 + VAT per quarter.

The Contract Term is 17 months (1.4 years), and the Bidder starts to deliver services (and therefore Social Value) in the 3rd month of the contract. They would therefore be eligible for SVP fees for 14 months. The first four quarterly invoices would be for £1,125 + VAT and the final invoice would be pro-rata at £750 + VAT.

**Example B: 37 Months - £80M**

A Contract is £80M, and therefore be subject to the maximum annual fee cap of £7,500 + VAT to use SVP. Fee’s are paid quarterly in arrears by direct debit after the point at which the Bidder starts to deliver social value at a rate of £1,875 + VAT per quarter. The Contract Term is 36 months (3 years), and the Bidder starts to deliver services (and therefore social value) in the 2nd month of the contract.

They would therefore be eligible for SVP fees for 34 months. All the quarterly invoices due to SVP would be for £1,875 + VAT, because the last year of the contract length is between 7 and 11 months, so fees will be rounded up to the next full yearly period(s).

SV Management Fee (excluding VAT):

| Total Contract Value (excl. extensions) | <£500k | £500k - £5M | >£5M |
| --- | --- | --- | --- |
| Annual SVP Fees | **£750** | **0.15%\*** | **£7,500** |
| Quarterly Payment | **£187.50** | **0.0375%\*\*** | **£1,875** |

\*0.15% of total contract value per annum

\*\*0.0375% of total contract value per quarter

## 

## 11.2.7 Finalising the Social Value Offer Post-Award

Following contract award the successful Bidder will need to agree with the Authority’s SV KPIs and the successful Bidder, using the Social Value TOM SystemTM to report on delivery and provide an approximate quantitative metric of the Social Value generated by the Contract.

To set agreed commitments on the selected Portal (currently Social Value Portal), the Bidder will need to attend a training session with the Authority’s Social Value partner (as noted before, Social Value Portal). Access to the portal will be given by the Authority and the Bidder will need to register with the portal in order to submit targets and record delivery of the SV Key Performance Indicators (KPI) throughout the life of the Contract.

Suppliers should note that Social Value proposals during the tendering stage, and subsequently the KPI’s agreed post contract award which will be chosen from those detailed in Appendix E, will be treated by the procuring authority as contractual commitments if the supplier is successful, and suppliers will be expected to report on delivery against these proposals at quarterly review meetings as part of contract management, using the Social Value Portal.

There may be genuine and justifiable reasons for the non-delivery of a Social Value offer from the winning contractor. In these circumstances the Authority will initially seek to engage with the winning contractor to determine what issues are impeding Social Value delivery. It will expect the successful supplier to have a coherent rectification strategy. This could include other Social Value proposals to an equivalent £ Social Value figure, if these also meet the Authority’s criteria.

# QUALITY

The Supplier must hold the following accreditations / certifications throughout the contract term. The winning bidder will be asked to provide valid certificates for the below prior to contract award:

* ISO 27001
* ISO 9001
* ISO14001

# PRICE

## Prices are to be excluding VAT and including all other expenses relating to Contract delivery. Table 7 summarises the charging options for each component of the service.

Table 7 - GovPrint Cloud component charging

| **Component** | **Charge option** |
| --- | --- |
| Cloud Service Normal Business House | Monthly Subscription on a per device basis |
| Cloud Services Extended Business Hours | Monthly Subscription on a per device basis when the optional extended business hours are applied. |
| Deployment Services - Client Onboarding | Price per client to onboard to the GovPrint Cloud service. Deployment prices must cover the provision of all services proposed to meet the requirements outlined in Sections 6.6.4 Client On-Boarding. |
| Development Services | Price per day for additional development, subject to agreed statements of work, based on the suppliers supplied SFIA rate. |

**Spend Discount Model**

Suppliers must enter the level of discount in Attachment 4\_Price Schedule within the ITT pack that will be applied as volumes increase over the contract term. Discounts will be applied to all connected devices on the month's invoice following the trigger of the following device volume bands, 10,000, 20,000, 30,000, 40,000, 50,000+.

**Other Pricing Requirements**

The Supplier must add any additional charges not factored in the above pricing model to the TBC section of Attachment 4\_Price Schedule within the ITT pack which will contribute to the Total Evaluated Price.

During the initial contract term (3 years), the contract charges shall be firm and are not eligible for variation. Should the Authority choose to undertake one or more of the optional extension terms then the charges in schedule 3 (Charges) will be increased in line with the D7BT - CPI -Consumer Price Index (CPI). The variation of price will be applied on day one of the extended contract term varying the price compared to the index 12 months prior.

**Development Services - SOW**

An example Statement of Work (SOW) for GovPrint Cloud development is available at Appendix C. Bidders are required to enter a price for completion of this statement of work within the Attachment 4\_Price Schedule within the ITT pack, detailing their SFIA role, daily rate (ex-VAT), and anticipated number of hours. The submitted price for this SOW will form part of the priced evaluation. The example SOW may be used by the Authority to form the first development activity following contract award, SOW001, however at the time of procurement the example is provided for pricing purposes only.

Any development required of the GovPrint Cloud service will be subject to agreement of each SOW using the SFIA rates supplied by the successful supplier in Attachment 4\_Price Schedule within the ITT pack. A template SOW is available at Appendix D.

# STAFF AND CUSTOMER SERVICE

The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.

The Supplier’s staff assigned to the contract shall have the relevant qualifications and experience to deliver the service to the required standard.

Key technical staff involved with implementing, managing or supporting the service shall have, or be expected to undertake National Security Vetting to Security Check (SC) level. All staff with Admin level access to the GovPrint Cloud Service must hold a valid SC Clearance.

Supplier staff who are required to have SC clearance must obtain the required clearances within three months of contract award, and must have, at minimum, Baseline Personnel Security Standard (BPSS) by contract award.

# SERVICE LEVELS AND PERFORMANCE

## Service Level Agreements

The following section outlines the core Service Level Agreements (SLAs) the Authority wishes to implement. The final Service Level Agreements will be fully documented in the Service Design.

**Definitions**

* Business Hours are Monday to Friday excluding applicable Bank Holidays 09:00 to 17:00
* Extended Business Hours are Monday to Friday excluding applicable Bank Holidays 08:00 to 18:00
* GovPrint Cloud Operational hours are 24 / 7
* The reporting period for all service metrics is one calendar month

**Service Levels**

| SLA Number | Description | Service Level Measure | Service Level Target |
| --- | --- | --- | --- |
| **1** | Cloud Services Uptime | Cloud Service fully functional 24/7/365. Agreed maintenance windows are accepted. | 99.99% |
| **2** | Fault Response and Resolution Time | Meet the response and resolution targets for all tickets.  First Time Fix Rate report shall be provided for information only | 97% of tickets resolved for P1  97% of tickets resolved for P2  97% of tickets resolved for P3  97% of tickets resolved for P4 |
| 3 | Software/Firmware updates and Release | Timescale to apply updates, or release client software | General Updates applied within 20 business days of agreed release  Security Updates applied within 2 Business Day for Critical and High Severity, and Medium and Low severity vulnerabilities updates applied as agreed, as defined by the Common Vulnerability Scoring System (CVSS)  Client software released within 8 weeks of OS or MFD release of update |
| 4 | Billing, Invoicing & MI Reporting | Provision of Invoice, Supporting Schedule and MI reports | 10 business days from period end |
| 5 | Change requests | Change request timeframe to be agreed for each change request | To be agreed on each change request |
| 6 | Client deployments | Deployment project timeline to be agreed for each deployment request | To be agreed on each deployment request |

**Response / Resolution Times**

|  | | Impact | | | |
| --- | --- | --- | --- | --- | --- |
| Critical -  Extensive impact across all locations and clients (total outage) | High-  High impact at a single site or more than 50% of a site’s users | Medium-  Impact for less than 50% of a site’s users | Low-  High impact limited a single user |
| Urgency | Critical -  stopping client from working | P1 | P1 | P2 | P2 |
| High -  Significant degradation of service | P1 | P2 | P2 | P3 |
| Medium -  Customer is inconvenienced | P2 | P2 | P3 | P3 |
| Service Request | P4 | P4 | P4 | P4 |

| Impact | Description | Initial Response | Target Resolution | Hours in Effect |
| --- | --- | --- | --- | --- |
| P1  Critical Impact / Urgency | * Service unavailable to all users * No possible workaround * Dept core functions severely impacted | 15 mins | 1 Hour | 24x7 |
| P2  High Impact / Urgency | * Service unavailable or severely degraded to majority of users * Service is usable but performance is severely impaired * Dept core functions impacted | 30 mins | 4 hour | 24x7 |
| P3  Medium Impact / Urgency | * Service unavailable or severely degraded to minority of users * Service is usable but performance is impaired * Dept core functions impacted | 1 hour | 8 hours | Business Hours |
| P4  Service Request | * Service request e.g. change request | As per specific service type | As per specific service type | Business Hours |

Examples of incidents and their associated priority include but are not limited to:

Cloud Service

Complete cloud outage across one or more sites - P1

Complete cloud outage across multiple tenancies - P1

Complete cloud outage across one tenancy - P1

Significant degradation of cloud service across all locations - P2

Significant degradation of cloud service across multiple locations - P2

Significant degradation of cloud service across one location - P3

Minor degradation of cloud service across any site - P3

## 

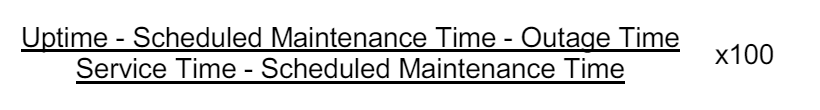
**Service Credits**

* Service Credits shall be applied where performance falls below the SLA target within a reporting period. The service credits are detailed in Schedule 10 (Service Levels)
* A critical service level failure shall be when one or more of the following occur:
  + Cloud Service Uptime <99.5% in any reporting month period
  + Fault Response and Resolution Time <90% in any reporting month period
  + failure to achieve the 99.99% ‘Cloud Services Availability’ threshold in three or more separate (consecutive or nonconsecutive) months during any 12-month rolling period; and/or
  + failure to achieve the required performance threshold for the ‘Fault Response and Resolution Times’ service level for Severity 1 Incidents in three or more separate (nonconsecutive) months during any 12-month rolling period; and/or
  + failure to achieve the required performance threshold for the ‘Fault Response and Resolution Times’ service level for Severity 2 Incidents in three or more separate (nonconsecutive) months during any 12-month rolling period; and/or
  + failure to achieve the required performance threshold for the ‘Fault Response and Resolution Times’ service level for Severity 3 Incidents in four or more separate (nonconsecutive) months during any 12-month rolling period

Performance will be managed in accordance with Schedule 10 (Service Levels) and where early termination takes place the supplier shall follow Schedule 30 (Exit Management Plan).

**Service Credits - Availability**

The availability of the service will be measured per calendar month according to the following uptime calculation:



# SECURITY AND CONFIDENTIALITY REQUIREMENTS

## General Approach

Schedule 16 - Security details the security terms where Part B applies.

All proposed products and services including cloud based services must provide adequate protection against cyber-attack, unauthorised disclosure of information and unauthorised access.

The supplier will ensure that all services are developed in line with recognised security good practice as set out by respected security organisations including but not limited to: the National Cyber Security Centre (NCSC); the US National Institute of Standards & Technology (NIST); the Centre for Internet Security (CIS); and the Open Worldwide Application Security Project (OWASP).

On an ongoing basis the supplier will be responsible for working with the Authority in a collaborative way to manage the security risks of the service commensurate with the obligations in the security schedule of the contract.

The Supplier will be required to demonstrate their compliance with relevant [NCSC guidance](https://www.ncsc.gov.uk/section/advice-guidance/all-topics) (<https://www.ncsc.gov.uk/section/advice-guidance/all-topics>) including the NCSC Cloud Security Principles (<https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles>) on the Authorities request for the Suppliers solution and any cloud services the supplier uses to perform the full service.

## Information Assurance

Information held within systems that can be used to print to the GovPrint service will be classified as OFFICIAL and all proposed hardware and software solutions must deliver a suitable level of protection.

Proposed solutions and services must comply with the UK Data Protection Act and any replacement data protection regime.

The Supplier and relevant subcontractors must hold and maintain ISO27001 accreditation for the full period of the Agreement.

The Authority will require the Supplier and relevant subcontractors to hold and maintain Cyber Essentials Plus for the service delivered.

The final solution agreed with the Supplier will be subject to review and agreement as part of the standard Authority Information Assurance process; the Authority will provide Information Assurance input and feedback to the supplier throughout the design and build process where reasonably requested to ensure a secure-by-design approach to service development and delivery.

The Supplier will ensure that the cloud print service is hardened against a recognised security benchmark (e.g. CIS), as agreed with the Authority.

The Supplier will ensure that the service is subject to regular (at least annual) IT Health Checks (ITHC) conducted by a (mutually agreed) qualified third party under the auspices of the NCSC CHECK scheme:

* These will be conducted periodically as part of on-going assurance, or at any point where the service is subject to a material change.
* The scope of testing and remedial action plans will be agreed with the Authority.
* All test documentation will be shared with the Authority including, but not limited to, scope documents, test reports and other outputs, remediation action plans and other supporting documentation.
* The Supplier will actively work with the IT Health Check service provider to support testing, develop remedial action plans and support remediation of identified vulnerabilities or risks.
* All findings must be treated to the Authority’s satisfaction on a timescale as agreed with the Authority; regular progress reports against remedial actions must be provided by the supplier.

The Supplier will employ measures to continually monitor the service for vulnerabilities:

* This will include a security dashboard or regularly updated security view, shared with the Authority, highlighting the threat management status and security patching status for all devices and other service components.
* Vulnerabilities will be patched on a schedule as pre-agreed with the Authority depending on criticality.
* The Supplier will immediately notify the Authority of any CRITICAL findings, via a mechanism pre-agreed with the Authority.

The Supplier will employ measures to continually monitor, prevent, detect and respond to any anomalous activity or indicators of possible compromise on the service:

* The Supplier will immediately notify the Authority of any event or activity which requires an immediate response to limit the impact of compromise, via a mechanism pre-agreed with the Authority.

The Supplier will provide a brief monthly report highlighting any security incidents and anomalous activity for the period and summarising new vulnerabilities, patching progress, trend analysis and other information of security interest.

The Supplier will restrict all management and other access to the service and its data to only those persons with a valid 'need to know':

* All access and activities will be attributable to the specific users who initiated them and enable non-repudiation of user actions.
* All access will be provided on a 'least privilege basis' so that the minimum level of access is provided to meet the business need.
* Access control lists will be regularly reviewed, and updated in line with JML processes so that individuals only have access during such time as their role requires it.
* The Supplier will retain accounting logs relating to management of the service in a format, and for a period, to be agreed with the Authority.
* Sufficient background checks will be conducted on all supplier personnel working on the service.

## Device Security

### Device Protection

Full definition of the security requirements of print devices connected to the GovPrint Cloud service is outside the scope of this document. However, the GovPrint Cloud service must support the following when connecting to print devices:

* Protection of data in transit using industry standard protocols such as HTTPS / TLS 1.3 or higher, this will include data in transit from client EUC devices to the Cloud Service and Print Devices to the Cloud Service
* X.509 certificates for device identity and cryptography. CA issued certificates issued and managed by the Supplier. For the avoidance of doubt, self signed certificates are not acceptable. Device certificates should be valid for one year, or for the expected life of the device on the network (whichever is shorter).

## NCSC Cloud Security Principles

The GovPrint Cloud service must support the [NCSC Cloud Security Principles](https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles) (<https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles>) and the supplier will be asked to demonstrate conformance with the principles:

* Cloud Security Principle 1: Data in transit protection
* The aim is to ensure data transiting networks is adequately protected against tampering and eavesdropping
* Data must be protected during transmission between any components of the service including:
  + EUC Client to Cloud secured using HTTPS (TLS 1.3 or higher)
  + Cloud to print device secured using HTTPS (TLS 1.3 or higher)
  + Email service using SMTPS / STARTTLS
* Support for suitable Key Exchange, Cipher and Data Integrity standards including
  + X.509
  + AES
  + SHA-2
* Implementation of TLS must comply with [NCSC’s guidance on using TLS to protect data](https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data) (https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data)
* Cloud Security Principle 2: Asset protection and resilience
* The aim is to ensure data, and the assets storing or processing it, are protected against physical tampering, loss, damage or seizure
* Physical location and legal jurisdiction - services that store, process or manage information must be provided in data centres located in the UK. Where any information is processed outside the UK the Supplier must clearly identify the information and the circumstances under which the information is processed e.g. to provide support or technical assistance. Where significant data processing occurs outside the UK the service will be deemed not to be fully compliant.
* Data centre security - locations used to provide cloud services must have adequate physical protection against unauthorised access, tampering, theft or reconfiguration of systems. These measures must conform to a recognised standard such as CSA CCM v3.0 or SSAE-16 / ISAE 3402
* Data at rest protection - the service must provide suitable protection of data at rest to ensure data is not available to unauthorised parties with physical access to infrastructure. This must include:
  + Physical access control
  + Encryption of physical media using suitable encryption standards such as AES
  + Infeasibility of finding a specific customer’s data on physical media
* Data sanitisation - the process of provisioning, migrating and de-provisioning resources should not result in unauthorised access to user data
* Equipment disposal - once equipment used to deliver the service reaches the end of its useful life, it should be disposed of in a way which does not compromise the security of the service, or user data stored in the service.
* Physical resilience and availability - the supplier must ensure that the service is designed and delivered to meet agreed service levels
* Cloud Security Principle 3: Separation between users
* The aim is to ensure a malicious or compromised user (organisation) of the service should not be able to affect the service or data of another
* The supplier must clearly document how separation of data between tenants is maintained by the service including logical separation within the software solution and/or the underlying infrastructure. This should include separation between users of the GovPrint Cloud service and other users of the underlying cloud service and separation between users within the GovPrint Cloud service (see 6.5.3)
* Cloud Security Principle 4: Governance framework
* The aim is to ensure that the service provider has a security governance framework, with board-level accountability, which coordinates and directs its management of the service and information within it
* The supplier must adopt and conform to common security standards such as CSA CCM v3.0 or ISO 27001
* Cloud Security Principle 5: Operational security
* The aim is to ensure that the service is operated and managed securely in order to impede, detect or prevent attacks.
* The supplier must operate the following:
  + Configuration and change management
  + Vulnerability management
  + Protective monitoring
  + Incident management
  + Major Incident Management
* Cloud Security Principle 6: Personnel security
* The aim is to ensure that supplier staff that have access to the service are trustworthy
* The Supplier must have suitable process for screening staff
* Key technical staff involved with implementing, managing or supporting the service should have, or be expected to undertake National Security Vetting to Security Check (SC) level
* Cloud Security Principle 7: Secure development
* The aim is to ensure that services are designed and developed to identify and mitigate threats to their security
* The service must be based on components that have been developed in an environment that considers security with an approach adheres to a secure development standard or recognised good practice
* Cloud Security Principle 8: Supply chain security
* The aim it to ensure that all suppliers involved in providing the service satisfactorily support all of the security principles required to provide a secure service
* All suppliers that provide the service must hold ISO 27001 accreditation
* Full traceability must exist for all elements and dependencies of the service.
* Cloud Security Principle 9: Secure user management
* The aim is to ensure that all clients can securely manage their use of the service
* The service must support:
  + Authentication of users and support role based access control
  + Protection of management interfaces and support channels
  + Admin access protected by Multi-Factor Authentication (MFA)
  + Separation and access control within management interfaces
  + Joiners, movers and leavers (JML) processes for through-life management of users
* Cloud Security Principle 10: Identity and authentication
* The aim is to ensure access to the service is limited to authenticated and authorised users.
* The service must ensure:
  + Identity is federated with the clients existing identity service
  + Only authenticated and authorised users have access to services based on their role
  + Users must be authenticated before using print devices and portals/interfaces
  + The service must support multi-factor authentication to management interfaces
* Cloud Security Principle 11: External interface protection
* The aim is to ensure all external or less trusted interfaces of the service should be identified and appropriately defended
* All service endpoints are protected including
  + Web interfaces are protected and only allow authenticated users to access the service
  + System end points e.g. print devices or software clients are protected using certificates
* Cloud Security Principle 12: Secure service administration
* The aim is to ensure that systems used for administration are adequately protected
* The Supplier must have a documented service management architecture that ensures system management limits privileged access to the service and limits risk
* Cloud Security Principle 13: Audit information for users
* The aim is to ensure that clients have access to audit records required to monitor access to the service and the data held within it
* The service must support comprehensive audit and reporting capability in line with GPG 13
* Clients must be able to access logging data for their tenancy and Authority must be able to access logging data for the full service
* Cloud Security Principle 14: Secure use of the service
* Authority will ensure that users of the service are adequately trained to use the service and the Supplier must support this as appropriate e.g. training, documentation etc.

## Security Policies and Procedures

### Information Security Management System (ISMS)

The Supplier shall develop and maintain an Information Security Management System (ISMS) that is compliant with the requirements set out in Schedule 16 (Security).

### Security Management Plan

The Supplier shall develop and maintain a Security Management Plan that is compliant with the requirements set out in Schedule 16 (Security).

### Security Incident Response Plan / Security Breach

The Supplier will implement a Security Incident Response Plan that is compliant with the requirements set out in Schedule 16 (Security).

### Vulnerabilities

The Supplier will manage vulnerabilities and fix them in accordance with the requirements set out in Schedule 16 (Security).

### Business Continuity and Disaster Recovery

The proposed solution must be resilient and secure. The Supplier must design the solution to be resilient with minimal single points of failure. The design must support the relevant SLA targets set out in section 15 Service Levels and Performance.

The Supplier must demonstrate they have a Business Continuity Plan for the GovPrint service and their organisation.

The Supplier must work with relevant parties to implement and test the Business Continuity Plan as per Schedule 14 - Business Continuity and Disaster Recovery.

# PAYMENT AND INVOICING

## Authority Locations

Authority recognises that the flexible nature of its requirements could lead to a complex billing process. The overall objective will be to work with the Supplier to implement a billing process that is simple and efficient.

In summary:

* The Supplier will bill Authority based on the agreed cost model
* Authority will recharge costs to clients based on client print volume

The Supplier must issue a quarterly invoice for all services delivered during the billing period. The structure and content of the invoice will be agreed between Authority and the Supplier based on the selected commercial model.

GovPrint Cloud subscription costs can be billed in advance and deployment services can be billed in arrears.

The Supplier must issue a detailed schedule in support of the invoice. This schedule will include both summarised data plus a record for each device that includes:

* Number of devices connected
* Print volume split by mono and colour per client

The Authority and the Supplier will work together during Service Design to agree on an appropriate format for the invoice and schedule.

The Authority will validate some or all volume data submitted as part of the billing schedule.

The Supplier must collect all information required for reporting automatically.

Invoices should be submitted to the address stated on the relevant Purchase Order and must reference the relevant Purchase Order number.

17.2 Payment can only be made against a valid Purchase Order.

Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

Before payment can be considered, each invoice must include a detailed elemental breakdown.

Amounts due under such invoice shall be payable within thirty (30) days after receipt of such invoice.

Invoices will be sent to: Government Property Agency, 23 Stephenson Street, Birmingham B2 4BJ Invoices and credit notes must be sent to this email: [gpaapinvoices@gpa.gov.uk](mailto:gpaapinvoices@gpa.gov.uk). For statements and queries: [financeoperations@gpa.gov.uk](mailto:financeoperations@gpa.gov.uk). You must be in receipt of a valid PO Number before submitting an invoice. To avoid delay in payment it is important that the invoice is compliant and that it includes a valid PO Number in the format of GPA xxxxx, your full company name and address, clearly addressed to the payee, and a unique invoice number. Invoices must be in PDF or Word format and each invoice should be on a separate attachment. Documents such as JPEG’s or excel do not constitute a valid invoice/credit therefore will be returned. If you are unable to email invoices, please post them to: Government Property Agency 23 Stephenson St, Birmingham B2 4BJ **Non-compliant invoices will be returned to you if they are not in the correct format.**

# CONTRACT MANAGEMENT

## 

## Service Delivery Management

Service Delivery Management (SDM) is central to delivery of benefits and the long-term success of the Shared Print Service.

The purpose of SDM includes but is not restricted to:

* Provide a defined communication route between Authority and the Supplier
* Service performance management / Service delivery management
* Benefits realisation
* Service planning – availability and capacity
* Product and technology review including product portfolio review
* Issue escalation
* Continual service improvement

**Structure**

The Authority will assign a named individual as the Contract Manager.

The Supplier will assign a named individual as the lead Contract Manager who will act as the key contact for Authority.

The Contract Managers will be responsible for the day to day operation of the service.

Where the service has been deployed outside Authority hubs / locations, Authority may also include the relevant government department in any service review meetings.

Authority expects that three levels of meeting will be required:

* Monthly Review
* Service performance review / Service delivery management
* Review open issues
* Quarterly Review (as above plus)
* Fleet design review – on-going fleet optimisation ensuring the right device in the right location
* Service planning
* Benefits realisation
* Continual service improvement
* Product and technology review including product road maps
* Catalogue management
* Annual Review (as above plus)
* Contract review

Due to the range of topics covered in the service review meetings a number of staff from both Authority (and relevant third parties) and the Supplier can attend the meetings as deemed appropriate.

All meetings must be fully documented by the Supplier.

Attendance at Contract Review meetings shall be at the Supplier’s own expense.

## End of Contract

At the end of the contract the Supplier must not impose any additional fees or costs including, for example, any costs for removal of equipment or settlement of contracts or leases.

Upon expiry, termination or cancellation of the contract it will be the Supplier’s responsibility for the removal of any hardware and software solutions at no cost to Authority.

The Supplier must ensure secure destruction of any customer data. Authority will require certification for each device that follows this process.

Upon expiry, termination or cancellation of the contract the Supplier must work cooperatively with Authority to ensure an orderly transition. This will include, but is not limited to:

* Provision of a full and accurate asset list with details of all hardware and software solutions deployed as part of the solution, including any associated transfer or termination costs
* Where any hardware or software solutions are to be removed, agree an appropriate and reasonable timescale for removal
* Where hardware or software solutions remain in use by Authority during any transition period beyond the end of the contract the prevailing contract costs will be applied for any print volume produced on the Supplier’s equipment.
* Support development of a Joint Exit Plan

Where any hardware or software solutions are removed by the Supplier any Authority and/or Tenant information must be securely removed and/or overwritten.

# LOCATION

The Authority reserve the right to deploy the service to:

* Authority locations
* non Authority locations.

Authority is not committed to rolling out the service to these specific hubs or any other locations.

The supplier will be required to work remotely or on site as appropriate.

# APPENDICES

# Appendix A - GovPass

**GovPass Standard**

## **Introduction**

GovPass cards can be used for a number of ancillary functions – this includes follow me printing applications provided by a third party i.e. printing documents.

There are two methods of integrating GovPass cards for RFID (radio frequency identification) based follow me printing applications – use of the ‘static’ card serial number and the more secure but formal DESFire card read using pre populated card applications that require initial authentication.

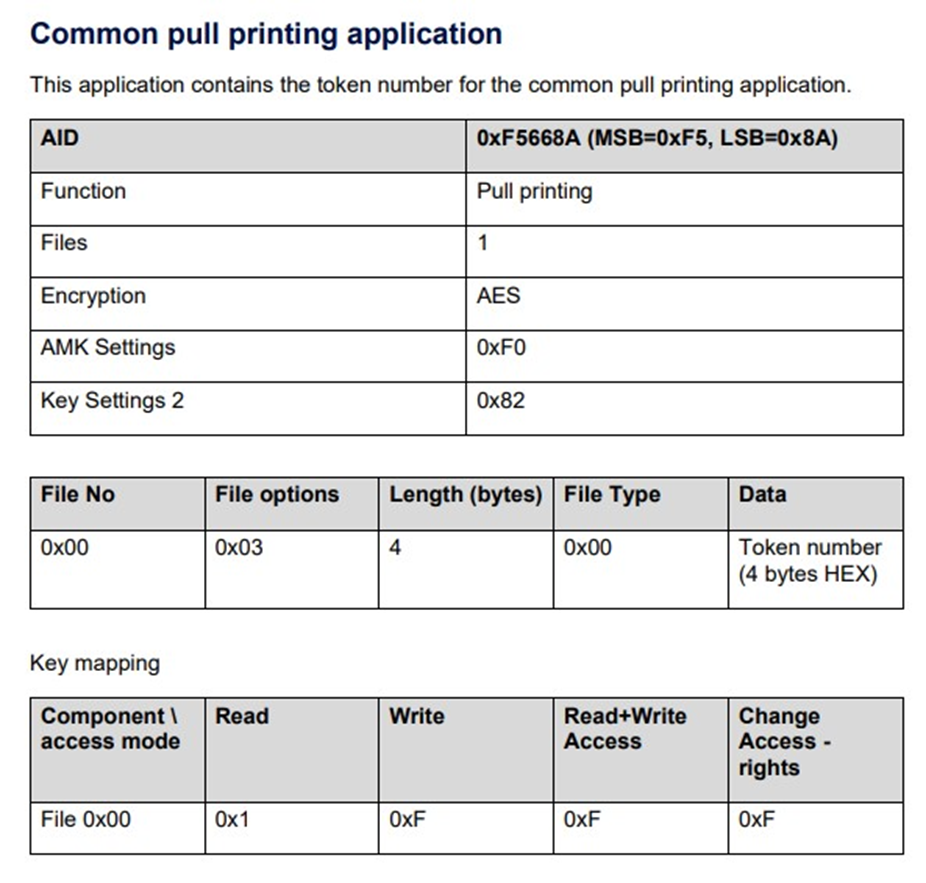
In terms of reader operation the solution shall always attempt to fully authenticate with the PPA1 card application first, then if unable to authenticate successfully, attempt to determine the card CSN (Chip serial number) or UID (Unique card Identifier), and if this fails then another credential if required by the Authority.

## 

## **GovPass PPA1 fully authenticated DESFire card read**

This allows the true card number to be electronically read and attributed to the card holder. Furthermore if an API call was instigated to the CHECK service, the card status can be provided that allows the print application to make informed decisions (please see GovPass API).

This method of card authentication will require a number of compatible (to ISO 14443A) reader configurations to be made and a static AES 128 key to be programmed into the printer card reader to allow the card to be read. The specification for conducting the fully authenticated card read is detailed in Fig 1.

**Fig 1 – ‘Follow Me’ printing card read specification using PPA1 Application** 

* Data offset: Nill
* Card SAK: 0x20
* Fully Enciphered communications

This method has the advantage that the unique GovPass card number is directly attributable to the number printed on the GovPass card, and the method for extracting the number is fully enciphered through a nominated GovPass application.

### **CMAC (Cipher Message Authentication Codes) secure messaging**

Currently a backward compatible EV1 card read is permitted (with no secure messaging), however solutions shall allow the invocation of full CMAC i.e. use of NXP "Secure Authenticate\_EV2" format, when this enforced at card level.

## **Use of GovPass CSN/UID**

GovPass cards comply with ISO 14443A & B and can provide a unique static card serial number (CSN), noting this is not the GovPass card number that is printed on the card. The GovPass CHECK service records the card CSN when the card is encoded and advice from the GovPass team should be sought when onboarding systems using this method.

The full 7 byte CSN should be utilised when appending a users rights against the printing application software, and preferably a API call should be made to CHECK (GovPass card management database that manages all card states: produced, enrolled, revoked, lost or building only card states). Where it is not possible to process the full 7 byte CSN i.e. where it is truncated by the reader, all enquiries should be directed to the Authority.

Note that the use of the card CSN (alternatively known as the UID – unique card identifier) is not considered secure as the CSN can be easily replicated.

## **Key Handling Policy**

With regards to Authority and Supplier handling of the encryption keys, this should be in accordance with any pre existing Departmental IT or ACSEC key handling policies that specify the minimum security standards for handling HMG assets but should include:

1. Keys shall only be transferred where it is essential to do so; the number of key transfers shall be kept to a minimum.
2. Keys shall only be sent to personnel with a need to know; there shall be non-repudiation of all parties to the transfer.
3. Recipients shall be notified in advance of when the transfer is going to take place; there shall be clear instructions for what to do if the key material is not received at the specified time.
4. Mechanisms enabling direct file transfer shall be used; keys shall not be emailed or sent over other mediums which might be either intercepted in transit or misdirected through user error.
5. Keys shall be protected in transit by robust file encryption (e.g. encrypting with a symmetric key and using the receiver's private key as a key-encrypting-key)
6. Cryptographically strong authentication of both the sending part and the receiving party shall be implemented (e.g. signing with the sender's private key and using the receiver's private key as a key-encrypting-key).
7. Keys shall be protected in transit by robust data-in-transit encryption (i.e. using NCSC-approved cipher suites)
8. Controlled access to keys shall be through ‘role based access’ or other controls to limit access to need to know groups only.
9. All suppliers/contractors handling such keys shall not store or send keys to any other party without permission from the Authority.
10. All suppliers/contractors handling such keys shall provide a process to delete all instances of key material as soon as they are no longer needed, and to provide an assurance, triage & recovery process that includes the immediate reporting of any key loss to the Authority in the event of a breach.
11. Any compromised keys shall be swiftly revoked and replaced.

The appropriate encryption key to access the printing application can be issued on request to the Authority, alongside the respective handling process.

Whenever possible, it is preferred to deliver key material to a pool printer RFID reader within an enciphered data packet contained within a pre programmed ‘configuration card’ that would be issued by the Authority. The target application identifier (AID) that contains the key material would need to be initially agreed between the parties together with the data packet and communications protocol (fully enciphered AES128).

## **Test Cards**

To allow a vendor to onboard GovPass cards, a request can be made to the Authority for provision of a test card set and/or a test PPA1 key that allows full testing of the vendors solution. Only upon written evidence of a successful test will the Authority release any live encryption keys.

Furthermore an API stack is available for testing the vendors solutions with the CHECK service – further details are available on request.

**GovPass API**

The GovPass service includes an AWS-hosted cloud based private API interface to enable services to confirm the validity of the GovPass card associated with the CSN (card serial number). The GovPass API infrastructure is private and only accessible via a Site-to-Site VPN and will require appropriate configuration by the supplier.

The following is extracted from the GovPass API Technical Documentation and relates to the **CheckCSN** API which the supplier would be required to interface with:

**CheckCSN Request Example**

**HTTP Method:** GET

**URL:** {{baseURL}}/CheckCSN?GovPassCSN=0490404A627180

* **{{baseURL}}** will be the URL for the API
* **CheckCSN** is the API resource used.
* **GovPassCSN** is the query parameter key.
* **0490404A627180** is an example GovPass CSN value, GovPass CSNs are 56 bit hexadecimal numbers. Some card readers output this value as a decimal number, if so, this must be converted to hex or it will fail the API's validation requirements.

**CheckCSN Response Example**

The following is the response to the example request detailed above. All responses are in JSON.

{

"GovPassCSN": "0490404A627180",

"CardState": "Active"

}

* **GovPassCSN** returns the CSN value originally requested
* **CardState** returns the current reported status of the corresponding GovPass.

Possible **CardState** returns detailed in Table 4 - CardState values.

Table 4 - CardState values

| **State** | **Description** |
| --- | --- |
| Active | An active GovPass that can be enrolled at other locations. |
| Produced | A GovPass that has been encoded but not issued to site. Should not occur at live sties. Should trigger an alarm. |
| Issued | A GovPass that has been issued to a site but not yet enrolled for the first time. Is the expected return for when personalising a pass locally. |
| BuildingOnly | Reserved for GovPasses allocated for use as visitor or contractor passes that should not be used for access to any other building. Should trigger an alarm if not owned by the requesting building. |
| Lost | The GovPass has been reported as Lost by its Issuing Building. Should trigger an alarm. |
| Expired | Where a GovPass’ validity date has expired i.e. the holder’s clearance or contract has expired/ended. |
| Inactive | A state reserved for future use where a pass has been disabled. Should trigger an alarm. |

For the purpose of GovPrint Cloud integration, Active and BuildingOnly card states are the only authorised ones. Any other state should deny the user access and trigger an alarm.

**Authentication**

Due to the vendor agnostic nature of GovPass, the APIs have been designed with the varying capabilities of the building access control system vendors. Client certificates were not appropriate for use due to the likelihood of incompatibilities between the AWS API Gateway and ACS’. As such each site or lateral service will have unique VPN credentials and will be allocated a unique API key. This API key is issued by the GovPass project team and must be included in the header of each request. They key and value are:

• x-api-key - API keys are alphanumeric and contain 40 characters.

Appendix B - GovPrint Cloud Interoperability

As outlined in section 6.4.6 Cloud Print Service Interoperability. The Authority expects interoperability to be delivered using API functions provided by the current Cirros cloud service and the Suppliers cloud service. This appendix provides a summary of the expected API capabilities required to support interoperability between the cloud services.

This appendix defines the following:

* Required API Functions
* Security Considerations
* Additional Considerations

**Required API Functions**

To deliver interoperability between cloud services APIs supporting the following functions are required.

* **Login:** This API serves as the entry point for user authentication. A user at a receiving service can authenticate and obtain an OAuth token. The main output of this stage is a user session OAuth token that can be used for subsequent API calls within the user session.
* **Logout:** This API is used to end the user session and ensure secure logout by invalidating the associated user session OAuth token.
* **GetPrintJobs:** This API is used to retrieve information about available jobs for the authenticated user. The OAuth token for the user session is used to authenticate the user. The requesting service can request information about jobs associated with the user. This information should include job title, cost, page count, application, and URLs for accessing preview images and the actual print job. This information is passed to the requesting service. The user can select the print jobs they need to release. The requesting service can then retrieve these print jobs using the OAuth token. The print jobs are then processed by the requesting service and released on the print device where the user initiated the login process.
* **ReleasePrintJob:** This API notifies the sending service that a print job is completed and should provide details of the final output e.g. number of pages printed and print device details. The sending service can record the print transaction and remove the job from the sending service.

**Security Considerations:**

* **Protection of data in transit:** all communication must be protected using TLS 1.2 or higher encryption for all API interactions.
* **HMAC SHA256 signature:** To ensure message integrity and prevent tampering, each message must include a UTC timestamp and an HMAC SHA256 signature generated using a shared secret provided by the sending service.

**Additional Considerations:**

* **Service scope:** access to copy and scan services on the receiving service are excluded from the current scope.
* **Print job security:** The document acknowledges that the security of print jobs passed from the sending to the receiving service is the responsibility of the receiving service. However, it highlights the assumption that adequate print job security measures are included in the current tender.

**Further Information:**

It is recognised that this appendix provides an overview of the requirements and further clarification at a later stage will be required.

Appendix C - Example Statement of Work

Statement of Work (SOW)

By [Successful Suppliers Name]

For The Government Property Agency (GPA)

Date xx/xx/xx

SOW 001

References:

<https://www.gov.uk/guidance/the-technology-code-of-practice>

<https://www.gov.uk/service-manual/service-standard>

<https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles>

<https://www.gov.uk/guidance/gds-api-technical-and-data-standards>

Introduction

This is an example SOW, which may be developed into SOW001 and form part of the contract. This is subject to funding .

[Successful Suppliers Name] will perform the design, development and implementation of the GovPrint Cloud Interoperability for the GPA that will be utilised by clients using the GovPrint service.

This statement of work is subject to the terms and conditions agreed within C1000862 - GovPrint Cloud.

Purpose and objectives

The purpose of this project is to establish interoperability between the supplier’s cloud print service and another Cloud Printing supplier’s solution.

The project objectives are:

* Design and implement a solution that is:
  + aligned with government principles and standards (see references)
  + aligned with industry best practice
  + meets all regulatory requirements (if any)
* Implement a bi-directional interoperability between the supplier’s cloud print solution and another nominated Cloud printing solution

Tasks

[Successful Suppliers Name] will complete the following tasks as part of this project:

* Discovery - Participate in the discovery process with GPA and the nominated Cloud Printing supplier to support the following key activities:
  + Review and define the requirements for interoperability
  + Define high level API requirements
* Design - work with GPA and nominated Cloud Printing supplier to support the following key activities:
  + Fully define the APIs required to meet the requirements defined during the Discovery phase (Low Level API Design)
  + Support GPA IA review of design
  + Fully document technical and service design
* Development - Implement agreed APIs in supplier’s Cloud service
* Testing - work with GPA and nominated Cloud Printing supplier to:
  + Configure interoperability between the cloud print services using the APIs
  + Complete functional testing
  + Complete non-functional / performance testing
  + Complete all remediation activities required
* Information Assurance:
  + Undertake ITHC based on scope defined by GPA
  + Remediate any issues found
* Transition:
  + Develop a transition to live service plan
  + Make interoperability services available in production environment
  + Pilot running of interoperability services
  + Remediate any issues found during pilot
  + Extend interoperability services to all clients

Deliverables

[Successful Suppliers Name] will provide the following deliverables as part of this project:

* Interoperability Requirements
* High Level API Requirements
* Low Level API Design
* Technical and Service Design
* Implement API Design
* Functional / Non Functional Testing
* Updated API based on test results
* ITHC / Information Assurance
* Remediation Plan and implementation
* Transition to Live Service Plan
* Pilot Service
* Production Service
* Support Documentation
* Project Management

Schedule / Payment Milestones

This project will follow the below estimated schedule, over a **maximum of 9 months**:

| **Task/project phase** | **Indicative Percentage of Payment subject to agreement** | **Est. start date** | **Est. end date** | **Est. hours required** |
| --- | --- | --- | --- | --- |
| Discovery | 10 % | [Start Date] | [End Date] | [Hours Required] |
| Design | 25 % | [Start Date] | [End Date] | [Hours Required] |
| Development | 25 % | [Start Date] | [End Date] | [Hours Required] |
| Testing | 10 % | [Start Date] | [End Date] | [Hours Required] |
| Information Assurance | 10 % | [Start Date] | [End Date] | [Hours Required] |
| Transition | 20 % | [Start Date] | [End Date] | [Hours Required] |

Location

The majority of work related to this project will occur remotely, however it is recognised the benefit of in-person engagement at an appropriate location with the UK. Any such expense or travel will not be reimbursed.

Budget, pricing, and payment schedule

The GPA has a total budget of £300,000 for this project, not to be exceeded.

[Successful Suppliers Name] will charge the following per deliverable. The suppliers SFIA rates are to be in accordance with those detailed within Schedule 3 (Charges):

| **Deliverable** | **Price** |
| --- | --- |
| Discovery |  |
| Design |  |
| Development |  |
| Testing |  |
| Information Assurance |  |
| Transition |  |

Resources

The GPA will have the following resources available to enable [Successful Suppliers Name] to complete this project:

* 1 x Product Owner
* 1 x Technical Architect
* 1 x Security Architect

New IPR

In accordance with Schedule 36 (Intellectual Property Rights), the following New IPR and/or specially written software will be created by the supplier as a result of completing the above deliverables:

* [New IPR or specially written software created]
* [New IPR or specially written software created]

Signatures

Signed and agreed to by:

| [Successful Suppliers Name]  Signee Name  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  [Date] | On behalf of the Minister for the Cabinet Office on behalf of the Crown represented by the Government Property Agency  [GPA Signee Name]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  [Date] |
| --- | --- |

Appendix D - Template Statement of Work

Statement of Work

By [Successful Suppliers Name]

For The Government Property Agency (GPA)

Date xx/xx/xx

SOW #000

Introduction

[Successful Suppliers Name] will perform [overview of work required] for the Government Property Agency. This statement of work is subject to the terms and conditions agreed within C1000862 - GovPrint Cloud.

Purpose and objectives

The purpose of this project is to [purpose]. The project objectives are [objectives].

Tasks

[Successful Suppliers Name] will complete the following tasks as part of this project:

* [Task]
* [Task]
* [Task]

The following tasks are not included in this project’s scope and will not be performed by [Successful Suppliers Name]:

* [Task]
* [Task]
* [Task]

Deliverables

[Successful Suppliers Name] will provide the following deliverables as part of this project:

* [Deliverable]
* [Deliverable]
* [Deliverable]

Schedule / Payment Milestones

This project will follow the below estimated schedule:

| **Task/project phase** | **Indicative Percentage of Payment subject to agreement** | **Est. start date** | **Est. end date** | **Est. hours required** |
| --- | --- | --- | --- | --- |
| [Task/Project Phase] | % | [Start Date] | [End Date] | [Hours Required] |
| [Task/Project Phase] | % | [Start Date] | [End Date] | [Hours Required] |
| [Task/Project Phase] | % | [Start Date] | [End Date] | [Hours Required] |

Location

The majority of work related to this project will occur remotely, however it is recognised the benefit of in-person engagement at an appropriate location with the UK. Any such expense or travel will not be reimbursed.

Budget, pricing, and payment schedule

The Government Property Agency has a total budget of [budget amount] for this project, not to be exceeded.

[Successful Suppliers Name] will charge the following per deliverable. The suppliers SFIA rates are to be in accordance with those detailed within Schedule 3 (Charges):

| **Deliverable** | **Price** |
| --- | --- |
| [Deliverable] | £0.00 |
| [Deliverable] | £0.00 |
| [Deliverable] | £0.00 |

Resources

The GPA will supply the following resources to enable [Successful Suppliers Name] to complete this project:

* [Resource]
* [Resource]
* [Resource]

New IPR

In accordance with Schedule 36 (Intellectual Property Rights), the following New IPR and/or specially written software will be created by the supplier as a result of completing the above deliverables:

* [New IPR or specially written software created]
* [New IPR or specially written software created]

Signatures

Signed and agreed to by:

| [Successful Suppliers Name]  [Successful Suppliers Signee Name]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  [Date] | On behalf of the Minister for the Cabinet Office on behalf of the Crown represented by the Government Property Agency  [GPA Signee Name]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  [Date] |
| --- | --- |

Appendix E - Social Value KPI’s

