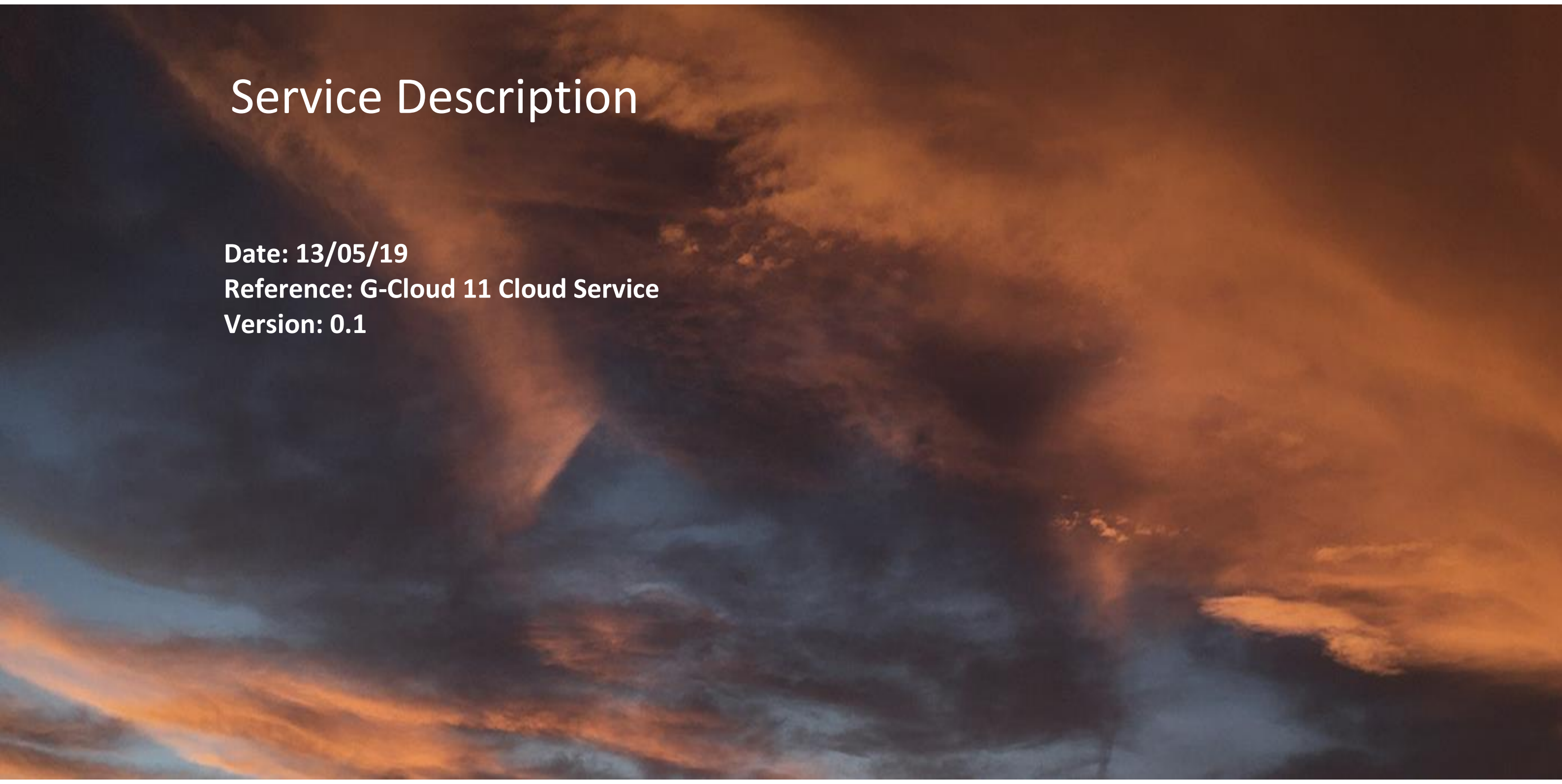

Service Description

Date: 13/05/19
Reference: G-Cloud 11 Cloud Service
Version: 0.1

DOCUMENT HISTORY

Version Number	Author	Description	Approval
V0.1	L Crick	First Draft	Rob Gittins

COPYRIGHT AND FREEDOM OF INFORMATION ACT

CONTACT DETAILS

The SecureCloud+ representative who may be contact in connection with this proposal is:

Louis Crick
Sales Team Manager
Greyfriars House, 30 Greyfriars Road, Reading, RG1 1PE
contact@securecloudplus.co.uk
+44 (0)330 123 3633

Table of Contents

1. COMPANY OVERVIEW

SecureCloud+ was founded in 2014 and we specialise in the delivery of innovative ICT systems for Defence and Public Sector customers with demanding security requirements, SecureCloud+ has grown its business through successfully securing and delivering several key government contracts providing end-to-end managed services at all tiers of the government's IT security classification system including up to TOP SECRET.

The Company has been awarded multiple key contracts with the MOD for managed services at all tiers of the government's IT security classification system. SecureCloud+ plans to deliver the same high level of service to organisations in the broader Public Sector.

SecureCloud+ is constantly seeking to leverage advances in technology to deliver modern ways of working whilst still exploiting the Government's investment in legacy systems. The Company's expertise in developing technological solutions, managing complex projects and protecting secure networks guarantees that services will be delivered to time and within budget.

The SecureCloud+ team have proven these principles in the delivery of critical systems in the UK and in support of Operations including the Middle East, Africa and Afghanistan.

2. SERVICE DESCRIPTON

2.1. Cloud Hosting

The SecureCloud+ Cloud Hosting Service is available at OFFICIAL (with a handling caveat of SENSITIVE), SECRET and TOP SECRET of the Government Security classification level. This scalable and elastic platform utilises a mixture of VDI and remote application technology supporting existing legacy, new and complex applications and services. SecureCloud+ has an integrated service portfolio, which enables its products and services to work coherently across all platforms including community, hybrid and private cloud and is designed to deliver the following capabilities:

- Consume raw compute and storage over secure networks.
- Develop applications in a secure sand-box environment.
- Provide access to, and storage of, information within or between secure networked environments.
- Store and collaboratively analyse requirements around multiple large data sets, raw and working files.
- Consume on-demand software applications.
- Access using networked client devices such as zero clients, desktops, laptops and tablets.

Provided as a fully managed service comprising comprehensive monitoring, analytics and log file processing in accordance with GPG13, the end-to-end service management is delivered as a full lifecycle methodology. The service can be provided either in UK or overseas locations.

2.2. Cloud Software

As part of its coherent and cohesive service portfolio SecureCloud+ can provide the following Cloud Software services in conjunction with its Cloud Hosting Services.

- Network Collaboration Service
- Managed Mobility Information Service
- Managed File Collaboration Service
- Managed Application Domain Service
- Managed Secure Domain Services
- Cyber Risk and Resilience Service
- Cyber Forensic Analysis Service
- Cyber Intelligence Analysis Service
- Predictive Workflow Analysis Service
- Information Exploitation & Analysis Service
- Digital Evidence Management Service
- Simulated Training Environment Service
- Secure Browse Service
- Secure Intelligent User Interface Service
- Secure Content Dissemination Service
- Data Visualisation for AI Service

- Digital Asset Management
- Deep Learning Forensics Service
- Digital Simulation Analysis Service
- Surveillance Analysis Service
- Predicative Asset Management Service
- Secure Blockchain Service
- Data Analysis & Interactive Reporting Service
- Cyber Simulation Training Service
- Command and Control (C2) Cyber Operations Service

SecureCloud+ offer Cloud Support services to customers to enhance, complement and support SecureCloud+ Cloud Hosting Services and Cloud Software Services detailed.

2.2.1. Cloud Support Service

Cloud Support Services are available to Customers to enhance, complement and support SecureCloud+ managed services detailed in Cloud Hosting and Cloud Software.

- DevOps as a Service
- Business Intelligence as a Service
- Cyber Consultancy as a Service
- Machine Learning as a Service
- Cloud Enabling Service

2.3. Methods of Delivery

SecureCloud+ are focused on delivering our services to Customers as quickly as possible following contract award. A project manager will be assigned and will be responsible for overseeing the transition of the service from its inception through to it becoming a live service. There is a robust transition process in place which utilises the concept of Service Gates to ensure that all key criteria for each stage of the project are fulfilled. This prevents the risk that vital tasks or information may be missed during the transition process.

A key component to ensure the success of any project is ensuring that a full discovery process is carried out to obtain a better understanding of the Customer's requirements. This can take the form of site surveys and interviews with Customer stakeholders with the aim being to produce a Statement of Requirement document that is signed off by both the Customer and SecureCloud+. This activity will take place as early in the transition lifecycle as possible. The Statement of Requirements document is then used as the basis to produce the service and technical designs and the associated test plans.

Once the requirement and solution are clear, SecureCloud+ will provide the Customer with a set of timelines and milestone dates that identify when each of the Service Gate stages are expected to be completed. If the Customer needs to access the solution earlier than the dates that the timelines indicate, SecureCloud+ will work with the Customer to provide an interim capability whilst the project is completed.

3. INFORMATION ASSURANCE

The secure managed service is delivered at the appropriate classification level.

- The service can support any additional requirements to interface with existing system monitoring equipment.
- All technical and service designs and supporting processes and documentation are in line with ISO9001, ISO20000 and ISO27001.
- All data centres used in the delivery of SecureCloud+ services are sited in the UK
- All delivery staff are UK Nationals, security cleared and based in the UK
- Service design and service provision comply with all Cloud Service Security Principles as directed by the Cabinet Office.

3.1. Accreditation

As part of its managed service, SecureCloud+ will work with its Customer and relevant stakeholders, including the appropriate Assurance bodies, to obtain the necessary accreditation and authority to operate. SecureCloud+ will own the following functional responsibilities:

- System Design Authority
- IT Security Officer

As part of the above responsibilities, SecureCloud+ will manage the following activities:

- Convening appropriate Security Working Group meetings
- Generating a complete Risk Management Accreditation Document set (RMADS)
- Preparing submissions to support an Authority to Operate
- Ensuring compliance with appropriate CoCo's and Cyber directives.

4. ON-BOARDING AND OFF-BOARDING

4.1. On-boarding

SecureCloud+ will initiate a formal project to manage the on-boarding process. The initial stages of the project will include Start-up, Project Management Plan (PMP) and Stakeholder engagement. There will be a mandatory Solution Discovery to:

- Ensure the service is the appropriate solution to meet the defined requirement
- Assess and evaluate any integration requirements of legacy services/applications
- Assess and evaluate any new capability requirements
- Establish access and delivery routes where appropriate
- Understand site specific service integration requirements
- Define specific security and clearance requirements
- Perform Health & Safety and Risk Assessments
- Define Critical Success Factors (CSFs) for User Acceptance Testing (UAT).

Following the Solution Discovery, the project will enter the design and detailed planning stage which will include project, technical and service delivery workshops. The output of these workshops will be to agree and establish the following:

- Project plan
- Communications plan
- Risk management log
  - Service Design Pack (SDP)Technical Design Documents
    - High Level Design
    - Low Level Design
  - Service Management Plan (SMP)
- Service transition plans for:
  - Migration
  - Testing and Acceptance
  - Training
  - Exit.

Implementation will follow the detailed planning stage where the service will be delivered against the SDP.

Test and acceptance tasks will be completed during the roll-out with the signed UAT denoting the point at which the service will be live and operational. All services provided by SecureCloud+ will enter a period of Early Life Support (ELS) following successful UAT where additional support, guidance and work instructions will be provided to the User.

4.2. Off-boarding

Six months prior to the termination or expiry of the contractual agreement SecureCloud+ and the Customer will engage in an Exit Plan. The Exit Plan will include a mandatory Termination Discovery which will define as a minimum:

- The method, format and return of Customer generated data most appropriate to meet the exit and security requirements
- Exit timetable and appropriate milestones for the return of hardware, software and other equipment
- The compliance requirements for secure destruction and sanitisation of media
- Health & Safety and Risk Assessments
- Service exit criteria.

SecureCloud+ will agree a price for delivering the Exit Plan and will have 10 days to transfer all Customer generated data residing within the SecureCloud+ solution. Upon termination date SecureCloud+ will ensure that all of the Customer data is deleted and destroyed in a secure manner.

5. SERVICE MANAGEMENT

5.1. Standard Service Packages

SecureCloud+ provides comprehensive service management packages; Core and Enhanced. Where there are specific service requirements which differ from the standard packages the requirement will be captured and priced during Solution Discovery.

	Standard Service Packages	
	Core	**Enhanced**
Service Desk	✓	✓
Service Cover	08:00-18:00 Mon-Fri excluding UK public holidays	24/7 Continuous
Service Request(s) Response Times	Catalogue defined and agreed based on User functionality	
Data Backup Recovery and Retention	Recovery Point Objective and Recovery Time Objective to be defined and agreed based on User requirement	
Disaster Recovery	To be defined and agreed based on Customer requirements	
Service Credit Regime	✓ up to 5% of Monthly Recurring Charge (MRC) in the service period	✓ up to 10% of Monthly Recurring Charge (MRC) in the service period
Solution Discovery	Mandatory	
Exit Discovery	Mandatory	
ITIL Service Lifecycle Management	ITIL Service Management including Incident, Problem and Change Management, Release and Deployment, Access Management, Availability and Capacity Management, Service Measurement and Reporting	
Management Reporting	Scheduled Service Reporting against SLAs, Project RAG Report	
Exclusions	*Availability based on Virtual environment; excludes customer network infrastructure and planned/emergency maintenance. Field Services outside of UK	
	Commercial Features	
Monthly billing in arrears	✓	✓
Quarterly billing in arrears	✓	✓
Electronic invoicing	✓	✓
Payment Options	BACS, Direct Debit, Debit/Credit Card, PayPal	

5.2. Service Level Agreements (SLA)

Network Collaboration Service		
Target Availability	99.95%	
Incident Response	Priority 1 within 30 minutes Priority 2 within 4 hours Priority 3 within 12 hours Priority 4 within 24 hours	
Incident Resolution	Priority 1 24 hours Priority 2 2 working days Priority 3 4 working days Priority 4 7 working days	
All other Cloud Hosting Services		
Target Availability	**Core**	**Enhanced**
	99.95%	98.90%
Incident Response	Priority 1 within 15 minutes Priority 2 within 4 hours Priority 3 within 12 hours Priority 4 within 24 hours	
Incident Resolution	Priority 1 8 hours Priority 2 16 hours Priority 3 24 hours Priority 4 48 hours	
Cloud Software		
Target Availability	**Core**	**Enhanced**
	Dependent on user requirements	Dependent on user requirements
Incident Response	Priority 1 within 15 minutes Priority 2 within 4 hours Priority 3 within 12 hours Priority 4 within 24 hours	
Incident Resolution	Priority 1 8 hours Priority 2 16 hours Priority 3 24 hours Priority 4 48 hours	

6. TRAINING

SecureCloud+ will provide appropriate training for Users of the service to ensure they are familiar with the capability, functionality and can therefore realise the benefits as quickly as possible. A training plan will be created at the Service Transition stage of the on-boarding process. The delivery of the training plan will include relevant User guides, appropriate use policies and work instructions as well as documented FAQs.

As part of the managed service delivery SecureCloud+ will maintain a KMDB and will suggest additional training as part of Continual Service Improvement.

7. ORDERING AND INVOICING PROCESS

7.1. Order Process

The accepted process for ordering this service and the Standard Service Packages is the standard G-Cloud process. SecureCloud+ will ensure the appropriate technical support is provided to assist the Customer in completing the Call Off order form.

7.2. Invoicing Process

SecureCloud+ will issue electronic and/or paper invoices monthly in arrears (or quarterly for Customers that order the Enhanced service option from the list of Standard Service Packages).

Payment terms are 30 calendar days from receipt of invoice.

8. TERMINATION TERMS

- Six months' notice of termination must be provided in writing to SecureCloud+ for the Managed Cloud Services.
- In the event of termination, all/any remaining service charges will still apply and will be payable on or before the termination date.
- Termination or expiry of the contractual agreement will initiate the Exit Plan as set out in the off-boarding section of this document. The Exit Plan will include a mandatory Termination Discovery.

9. CUSTOMER RESPONSIBILITIES

The Customer will be responsible for:

- **Local environment** – the environment, infrastructure and accommodation where the equipment will be located. This responsibility extends to power, cooling and moisture control.
- **Access to locations** – To arrange access to site for Security cleared contractors and SecureCloud+ personnel in order for them to discharge their duties in a timely manner.
- **Workplace Services** – Provision of permanent resources required to support the working environment of on-site engineers, e.g. desk, chairs, connectivity, local clearance.
- **Unit Request for Change** – the process and its overall management.

In addition, the customer must engage the appropriate Assurance bodies prior to engagement by SecureCloud+ delivery.

The service set out in this document is delivered at the appropriate Classification; it is the Customers' responsibility to ensure that any data stored and/or processed by applications within this environment is within the correct parameters.

SecureCloud+ will produce a Security Operating Procedure (SyOps) along with other information assurance requirements, the Customer must ensure all Users of the service observe and comply with these at all times.

Where the requirement incorporates access via third party secure networks (such as ALI, SLI, PSN, GSI, N3 etc) SecureCloud+ will define and demonstrate compliance with the relating Co-Cos but it is the Customers' responsibility to maintain the provision of access through the life of the service. It is also the customer's responsibility to advise of major changes in the underpinning networks and potential service interruptions. Where appropriate these may require change processes to be implemented.