Jupiter

Service Definition Document

Authored by: SecureCloud+

SecureCloud+

Table of Contents

Company Overview

SecureCloud+ Limited was founded in 2014 and specialises in the delivery of innovative, secure ICT systems for Defence and Public Sector customers with highly demanding security requirements. The company has grown through the successful award and delivery of key government contracts, establishing a strong reputation as a trusted provider of end-to-end managed services across all tiers of the UK Government security classification framework, including TOP SECRET.

SecureCloud+ continuously leverages advances in technology to enable modern, secure ways of working, ensuring services remain resilient, current, and scalable throughout their lifecycle. With deep expertise in solution design, secure service management, and complex programme delivery, SecureCloud+ consistently delivers high-assurance services on time and within budget.

The SecureCloud+ team brings extensive experience delivering mission-critical systems in sensitive environments, underpinned by rigorous governance, strong technical assurance, and a commitment to operational excellence.

1. SERVICE DESCRIPTION

Secure Defence Collaboration – Collaborative Working Environment

JUPITER is a centrally governed, secure, multi-service collaboration platform that enables assured collaboration across Defence and Public Sector organisations. It provides a unified entry point for accessing multiple collaborative projects through discrete Collaborative Working Environments (CWEs), with core capabilities including secure video conferencing (VTC), chat, and document management. These services are securely accessible from remote nodes across the consuming organisation's estate.

Each CWE is protected by end-to-end security controls, ensuring the secure handling, segregation, and protection of all data entered, shared, and stored. Where required, tiered separation is enforced to maintain strict information boundaries between projects and organisations.

Designed for scalability and cost control, JUPITER leverages modern compute infrastructure, automation, and Infrastructure as Code to deploy and operate services efficiently. Resources are dynamically allocated to each customer environment, with additional capacity provisioned seamlessly as demand increases.

JUPITER supports rapid onboarding to an assured, secret-classified network, enabling secure collaboration across dispersed user communities. Organisations are provisioned with dedicated organisational units and project-based CWEs, allowing them to operate independently or collaboratively as required. Each organisation is assigned a dedicated subdomain within the platform's Identity and Access Management (IDAM) framework, enabling independent user administration and access control while operating within a shared governance model. User Principal Names (UPNs) align with organisational conventions to ensure clarity and consistency.

Users participating in multiple projects can securely access all authorised CWEs through a single access portal over a high-grade cryptographic network. Optional, non-persistent unified communications can be enabled between organisations, without exposing or storing project data in the shared access layer.

All collaboration services, tools, processing, and data storage are contained wholly within the relevant project CWE. The organisational layer provides identity and access grouping only and does not host data or perform data processing, ensuring strict separation and assured information governance across the platform.

JUPITER Advanced Collaboration Service

JUPITER Advanced Collaboration Services (ACS) provide a secure, scalable platform designed to support Digital Engineering and other data-intensive defence activities. Delivered on a resilient core architecture, ACS supports a wide range of advanced applications and workloads, operated through a unified management layer to ensure consistent governance, flexibility, and operational efficiency.

ACS enables secure collaboration across disciplines through integrated capabilities such as 3D design, programme management, and Product Lifecycle Management (PLM). These services support collaborative engineering workflows, improve integration across complex delivery teams, and enhance transparency and control across programmes and projects.

Complementing ACS, High-Performance Computing (HPC) services provide the computational capacity required for digital test and evaluation, computational modelling, and advanced analytics. HPC resources are securely integrated into the JUPITER platform, enabling large-scale simulation, accelerated processing, and faster insight generation.

Together, ACS and HPC form an integrated Digital Engineering collaboration environment, enabling high-assurance collaboration, improved technical outcomes, and scalable performance across engineering and operational use cases, while maintaining strong security controls and cost-effective delivery.

Jupiter User Cases

JUPITER caters for a wide range of use cases which all follow the same architectural topology and underlying infrastructure principles.

Use Case 1 – A single shared physical platform. Hardware is shared to improve cost and delivery efficiency, with projects separated through platform controls where logical isolation is sufficient.

Use Case 2 – A shared Common Access, with separate hardware for CWE, to meet requirements for physical isolation.

- Shared storage array: separation is achieved logically and cryptographically within the common storage.
- Dedicated disks within a shared storage array; separation is achieved physically and cryptographically within the common storage.

Use Case 3 – A standalone stack with a separate Access Layer and dedicated physical hardware for a single project. Provides physical isolation from shared infrastructure while still using standardised build, configuration, and a shared management approach.

Use Case 4 – A fully independent, private instance of the entire technology stack tailored to a single customer.

2. DELIVERY

SecureCloud+ is committed to mobilising services rapidly following contract award. A dedicated Project Manager will be appointed to lead the transition from initiation through to live service, providing clear governance, coordination, and stakeholder management throughout delivery.

Transition is managed through a structured Service Gate framework. Each gate defines required inputs, deliverables, and acceptance criteria, ensuring the programme progresses in a controlled manner and reducing the risk of missed activities, dependencies, or assurance requirements.

Early in the lifecycle, SecureCloud+ will conduct a focused discovery phase to confirm operational, security, and technical requirements. This typically includes site surveys, stakeholder interviews, and collaborative workshops. Outputs are captured in a jointly agreed Statement of Requirements, formally signed off by both the Customer and SecureCloud+. This document provides the baseline for service and technical design, implementation planning, and the associated test and assurance plans.

Once requirements and the solution approach are confirmed, SecureCloud+ will provide an agreed delivery plan with key milestones, Service Gate dates, and clear responsibilities. Progress is tracked against this plan, with regular reporting and issue/risk management to maintain momentum and transparency.

Where a customer requires earlier access than the baseline plan allows, SecureCloud+ will work collaboratively to deliver an interim capability, enabling early operational benefit while the full service is completed and transitioned into business-as-usual support.

2.1. Secure-by-Design

SecureCloud+ brings over a decade of proven experience delivering security assurance across Defence IT systems and networks, spanning OFFICIAL through to TOP SECR*T classifications. Our approach is a clear Delivery Commitment to operational excellence, sovereign capability, and trusted partnership, ensuring resilience and confidence throughout the security lifecycle.

Security within JUPITER is not asserted; it is engineered through SecureCloud+ Secure-by-Design (SbD) Framework, aligned to MOD JSP 440 Leaflet 5C, NCSC guidance, and NIST 800-53. The framework is structured around seven core principles: understanding context, planning activities, managing risk, defining controls, engaging the supply chain, verifying assurance, and enabling through-life management. These are mapped to NIST PREPARE activities to ensure mission focus, clear system boundaries, and defined stakeholder responsibilities.

JUPITER is architected with security as a foundational requirement, applying Secure-by-Design and Zero Trust principles across devices, virtual environments, and operational practices. The platform, including end-user devices, is assured to store and process information up to SECRET, including International SECRET and UK SECRET UK EYES ONLY, maintaining strong data protection and system integrity at all times.

The implementation of Secure by Design (SbD) is intended to secure capabilities through continuous risk management. Ensuring that MOD capabilities are secure by design is crucial in achieving Defence Outcomes.

Implementation of SbD will produce the following outcomes:

- Threats are understood and security weaknesses are identified earlier in a project lifecycle, reducing costs and risks to delivery.
- Capabilities are more secure.
- Through life development and delivery of capabilities is more secure.
- Capabilities are enhanced by applying modern cyber security practices.

This workstream will initialise the discovery of information in preparation of accreditation and ongoing assurance activities including initial drafting of Technical Readiness Review Assessment (TRRA) for the Network Technical Authority, Release and Deployment Board in support of the JSP 604 rule set.

SecureCloud+ is experienced in delivering fully accredited/assured managed services to several government agencies, particularly the MOD. Based on this experience, SecureCloud+ recognises early engagement with the appropriate assurance leads is critical as part of the 'Prepare' phase under SbD, with security being at the forefront of the technical and delivery strategy.

SecureCloud+ assign the following Roles and Responsibilities to the Secure by Design approach:

- Capability Sponsors - Responsible for the sponsorship of the capability, its requirement development, concept of operation and ensuring the capability can address the risks in service.
- Senior Responsible Owners (SROs) - Accountable for the delivery of cyber secure outcomes throughout the capability lifecycle.
- Delivery Team Leaders - Responsible for the development and delivery of secure capabilities that support Defence Outcomes throughout the capability's lifecycle.
- Capability Owners - The in-service owners of the capability, responsible for operating the capability to support Defence Outcomes.
- Commercial Officers - Responsible for the implementation of contract terms and conditions in the MOD that ensure that security is enforced throughout the capability's lifecycle.
- Delivery Team Security Leads - The individuals within the Delivery Team responsible for advising Delivery Team Leaders on security and risk management.
- Cyber Security Assessor - Responsible for independent assessment of Delivery Teams' adherence to Secure by Design and relevant risk and security policies and standards. They coordinate between Delivery Teams dealing with similar security challenges to optimise solutions and minimise duplication of effort; and are responsible for consistent and coherent advice and support to relevant capabilities.

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 ATT, IATO and ATO
- Ensuring compliance with appropriate CoCo's and Cyber directives

2.2. Security 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.

SecureCloud+ will bring cyber and security SME expertise and experience to the Customer working across complex security architectures, with a sound understanding of information security practice and Government/NCSC security standards underpinned by our Quality Management System, including:

- ISO 9001:2015, ISO 20000-1:2018 and ISO 27001:2017
- NIST Cybersecurity Framework (CSF)
- NIST 800-37 and associated Security and Privacy Controls NIST 800-37
- Cyber Essentials Plus
- NCSC 14 Cloud Security Principals
- NCSC Good Practice Guide (GPG13) – Protective Monitoring
- NCSC 10 steps to Cyber Security Levels
- Relevant Joint Service Publications (604/440/etc.)

During the early service delivery phase, the security team will work closely with the Customer in the proposed security approach, to ensure a comprehensive assessment and delivery of the relevant security evidence. SecureCloud+ proposes to lead and engage with the Customer in the following activities:

- Convening and attending appropriate Security Working Group meetings.
- to the Secure-by-Design, continuous risk management process.
- Generate automated Security Operating Procedures (SyOps) for the user community.
- Ensuring compliance with appropriate Code-of-Connection and Cyber directives.
- Completing and apprising threat and vulnerability assessments.

- Performing, using assured 3rd party suppliers, IT health and vulnerability checks across all solutions and platforms.
- Preparing documentation and technical responses in support of MOD JSP 604 submissions to support an Authority-to-Operate (AtO).

SecureCloud+ will leverage our experience and expertise with the UK StratCom Cyber Defence and Risk teams and engage with CySAAS to ensure that all designs, processes, and implementations are carried out in accordance with the latest MoD guidelines.

Outcomes:

- Establish, develop, and maintain all relevant system Security Design Documentation.
- Engage with all relevant MOD authorities such as CySAAS and MoD Design Authority, JSP604 Case Officers.
- Complete the DART entry (presently still required by SbD until CATT has been formally released).
- Define workstream for any cryptographic requirements, responsibilities and sponsorship.

3. ON-BOARDING AND OFF-BOARDING

3.1. 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

- RAID (Risks, Assumptions, Issues and Dependencies) Log
- Service Design Pack (SDP)Technical Design Documents
- High Level Design
- Low Level Design
- Service Design

Service transition plans for:

- Migration
- Testing and Acceptance
- Training
- Exit Strategy and Plan

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) which will include UAT, additional support, guidance, and service user guides being provided for the Users. Following successful UAT the service will move into Live Operations.

3.2. Off-boarding

Six months prior to the termination or expiry of the contractual agreement SecureCloud+ and the Customer will engage in the creation of an Exit Plan. The Exit Plan will detail the actions that need to be completed to terminate the Service.

This will include:

- Notification to Case Officer and Accreditor that the service will be terminated
- The method or format of data transfer or destruction in line with System Assurance requirements
- Decommissioning of any physical infrastructure installed at the customers premises
- Supplier resources assigned to the support of the Service will be reassigned once the Service Termination actions have been completed.
- Confirmation of target dates for each action and the resources required to carry out the actions. The resources are likely to be required from both the Supplier and Customer organisations.
- Customers sign off, of the plan and authorise the Supplier to commence the exit process on the agreed date.
- Health & Safety and Risk Assessments
- Service exit criteria.

The exit plan will also highlight the expected costs covering elements such as:

- Asset removal
- Data destruction
- Unexpired value of deprecated asset not covered in contract value
- Resource required to accomplish transition/knowledge transfer

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 the Customer data is deleted and destroyed in a secure manner.

4. SERVICE SUPPORT OVERVIEW

SC+ Service Management policy and accompanying practices are aligned to ITIL(V4) Best practice principles and certified to ISO 20000-1 Service Management standards.

Core Service Management principles are focussed on meeting needs and achieving customer satisfaction through ongoing collaboration with service consumers, a holistic approach to service management and continual service improvement culture focussed on evaluation and enhancement of services to meet customer needs.

Standard Support

- Service Hours: 08:00 – 18:00 Mon-Fri UK
- SOC: 24*7*365 Monitoring and Response

Additional offering

- Extended Support hours available, dependant on requirements.
- Enhanced SLA's dependant on technical solution.

Service Levels

Standard Service Offering

Priority	Business Impact	Incident Response Time	Incident Resolution Time
1	• An Operational Emergency • A serious security incident • Total loss (all sites) of one or more Essential Services *	Within 30 Working Minutes	24 Working Hours

2	• Direct impact on one site which prevents the use of a unique program or Essential Service whereby individuals are consequently unable to continue work or carry out any further processing • A minor security incident	Within 4 Working Hours	48 Working Hours
3	• Direct impact on one User who can work utilising another device • A fault which prevents the effective use of any service and affects a substantial number of devices or users in one area or department	Within 12 Working Hours	72 Working Hours
4	• Service Requests	Within 24 Working Hours	72 Working Hours

4.1. SLA Dependencies

Where an SLA has failed due to the activity of an external Resolver Agent (RA), the SLA failure shall not be attributable to the SecureCloud+ Service. External RAs could include but are not limited to:

- Individual Site Internet Service Providers
- Power Failure

In the event of a predicted breach of Service Level Agreement (SLA) during the Incident Management process (or in exceptional circumstances that require direct escalation) the Escalation Management process can be invoked by either the Customer or SecureCloud+.

After logging the Incident, Functional (technical) Escalation will commence automatically if the Incident cannot be resolved at first line. The Functional Escalation process will move the Incident through second line/third line/System Design Authority support to the point of resolution and recovery.

Resolution and recovery should be met within the SLAs as described in section, Priorities, Acknowledgement and Resolution. If this is not the case and SLAs are breached, then Hierarchical (management) Escalation can be invoked alongside Functional Escalation.

5. TRAINING

Utilising our dedicated training team within SecureCloud+ the company 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 needs analysis will be undertaken during the design phase of the project, and a training plan will be created to facilitate the delivery. The delivery of the training plan will include

face to face, remote, or self-guided training (as required), along with 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 Knowledge Management Database (KMDB) and will suggest additional training as part of Continual Service Improvement.

6. ORDERING AND INVOICING PROCESS

6.1. 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.

6.2. 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.