# How UKCloud implements NCSC Cloud Security Principles

The Government Security Classification Policy (GSCP) requires cloud service customers to properly assess the security capabilities of potential cloud service suppliers, to satisfy themselves that their data will be appropriately protected..

This document details how UKCloud has implemented each of the 14 Cloud Security Principles through specific reference to the NCSC Cloud Security Principles Implementation Guide.

UKCloud's assured cloud solutions have been specifically designed to meet the needs of the UK public sector, delivering UK-sovereign services that are easy to adopt, easy to use and easy to leave, with genuine pay by-the-hour consumption models. UKCloud is a certified Public Services Network (PSN) service provider and N3 Aggregator, and its full range of services are regularly assessed and accredited by many Government Accreditors.

There's a lot of information and guidance available. We're here to help.



**Pure Commitment.**
**T** 01252 303 300
**ukcloud.com**

## Cloud Security Principle 1 — Data in transit protection

### UKCloud Assured OFFICIAL Cloud

- TLS- (version 1.2) or SSL-encrypted sessions protect UKCloud services such as access to the UKCloud Portal
- Native internet connectivity is provided; customers can deploy their own VPN (e.g. commercial grade), SSL/TLS or similar to protect their application over the internet
- Customers can also connect via trusted networks (e.g. PSN, N3/HSCN, Janet, CAS(T) circuits)
- Traffic between UKCloud's data centres is protected using NCSC-assured (CAS(T)) dedicated fibre circuits
- Secure API proxy service protects exposed vendor APIs

### UKCloud Elevated OFFICIAL Cloud

- TLS- (version 1.2) or SSL-encrypted sessions protect UKCloud services such as access to the UKCloud Portal
- Additionally, connections are available only via trusted networks, not directly from the internet
- Trusted networks include government community networks (PSN, RLI and legacy networks such as GSI), private networks (e.g. CAS(T) with CPA encryption), or an assured VPN gateway such as the UKCloud Secure Remote Access service. For clarity, direct internet connections are not available
- Traffic between UKCloud's data centres is additionally protected via CPA foundation-grade encryption over NCSC- assured (CAS(T)) dedicated fibre circuits
- Secure API proxy service protects exposed vendor APIs

## Cloud Security Principle 2 — Asset protection and resilience

### UKCloud Assured OFFICIAL Cloud and UKCloud Elevated OFFICIAL Cloud

- UKCloud services are hosted in multiple UK data centres, adjacent to out UK operations centres, and separated by more than 100 km for excellent geo-resilience while maintaining UK sovereignty
- All UKCloud data centres are subject to regular rigorous periodic inspections and independent validation of their security controls (e.g. physical perimeter, manned guarding, CCTV, access control systems, etc.) by NCSC and other Government Accreditors
- The data centre infrastructure and facilities are regularly assessed, and approved for all levels of information classification.
- Our highly secure data centres, which are subject to extensive external assessment, additionally benefit from extensive resilience across electrical, power, cooling and connectivity services — eliminating all single points of failure
- Within each data centre, the actual cloud platform is deployed using enterprise-grade infrastructure. Single points of failure have been eliminated using techniques such as load balancing, clustering, RAID and dynamic routing
- UKCloud is a UK-registered company operating entirely within the jurisdiction of UK law. All customer data is, therefore, processed in compliance with all applicable UK law including the Data Protection Act 1998. We are well advanced in our preparations for full compliance with the EU General Data Protection Regulation (GDPR) from May 2018
- Independent IT Security Health CHECK tests validate the physical security of the compute, storage and networking infrastructure, and that data is securely and irrevocably deleted when it is no longer required by customers
- UKCloud operates a Data Destruction Policy which ensures that storage media which has contained customer data is securely stored in a media safe pending its secure sanitisation or physical destruction (e.g. via assured components such as Blancco or Tabernus)

## Cloud Security Principle 3 — Separation between consumers

### UKCloud Assured OFFICIAL Cloud

- A UK-sovereign public cloud platform exclusively for public sector organisations and their industry partners, but accessible by the public to support citizen-facing digital services
- Network separation between different customers is achieved via customer-managed virtual firewalls which are configured to block all access by default
- Compute and storage separation is achieved via VMware Hypervisor technology which has been extensively used and tested across government systems
- Successful NCSC Design Reviews of the architecture ensuring effective and robust separation between customers
- Effective separation between customers has been independently tested by an NCSC-approved CHECK test provider which supports the independent assurance of this platform

### UKCloud Elevated OFFICIAL Cloud

- A UK-sovereign public cloud platform exclusively for public sector organisations and their industry partners. Sometimes referred to as a community cloud. Customers are required to comply with the relevant Code of Practice which ensures a good level of hygiene within the community relating to internet-facing public clouds
- In addition to customer-managed virtual firewalls, UKCloud manages a separate firewall platform which further isolates customers from each other
- Separation is further enhanced via assured components (e.g. CPA-approved VPN gateways such as Secure Remote Access and the Cross-Domain Security Zone)
- Successful NCSC Design Reviews of the architecture ensuring effective and robust separation between customers
- Effective separation between customers is achieved at multiple layers and has been independently tested by an NCSC-approved CHECK provider which supports the independent assurance of this platform

## Cloud Security Principle 4 — Governance framework

### UKCloud Assured OFFICIAL Cloud and UKCloud Elevated OFFICIAL Cloud

- UKCloud's governance and assurance framework is led by the Director of Compliance and Information Assurance
- UKCloud operates a mature and robust information security governance framework aligned to ISO27001 and ISO27018 as well as other relevant international standards
- The UKCloud governance framework aligns with the controls within the Cloud Controls Matrix (CCM) published by the Cloud Security Alliance (CSA)
- UKCloud additionally holds PSN accreditation for both the Assured service and the Protected (encrypted overlay) service, which requires full compliance with a significantly more detailed framework of controls mandated by the UK government via NCSC
- UKCloud's governance framework has been reviewed by HSCIC for UKCloud to act as an authorised N3 Aggregator

## Cloud Security Principle 5 — Operational security

UKCloud Assured OFFICIAL Cloud and UKCloud Elevated OFFICIAL Cloud

- UKCloud's operational security activities are regularly assessed and independently validated by a UKAS-accredited audit body and multiple Government Accreditors
- Additional assurance and independent validation are provided through UKCloud's ISO20000 IT Service Management certification and relevant independent vendor-based standards
- Experienced, trained security analysts identify, assess and respond to key threats and vulnerabilities detected by the UKCloud protective monitoring service
- These aspects have previously been independently validated by NCSC Pan Government Accreditation, and continues to be regularly assessed by Government Accreditors
- UKCloud has ongoing PSN accreditation for both the Assured service and the Protected (encrypted overlay) service
- UKCloud notifies security incidents to statutory organisations such as GovCERT and CareCERT, and has established protocols to work with organisations such as CERT-UK and CISP (Cyber Security Information Sharing Partnership) and sector-based WARPs (Warning and Advisory Reporting Points)

## Cloud Security Principle 6 — Personnel security

UKCloud Assured OFFICIAL Cloud and UKCloud Elevated OFFICIAL Cloud

- All UKCloud employees are required to maintain Baseline Personal Security Standard (BPSS) to verify their identity and their right to work, and disclose details of unspent criminal convictions
- All operational staff with access to the UKCloud Platform and operational facilities are required to maintain Government Security Check (SC) level clearance, as well as NPPV (Non-Police Personnel Vetting) at Level 3 for working with police organisations
- These requirements exceed the requirements of BS7858:2012
- All employees have signed the Official Secrets Act and benefit from regular information security education and training
- These aspects have previously been independently validated by NCSC Pan Government Accreditation, and continues to be regularly assessed by Government Accreditors

## Cloud Security Principle 7 — Secure development

UKCloud Assured OFFICIAL Cloud and UKCloud Elevated OFFICIAL Cloud

- UKCloud follows an agile development methodology which allows us to quickly adapt to changing security requirements and application development best practice
- Security threats are regularly reviewed, and patch creation and implementation is given the highest priority
- UKCloud undertakes thorough security testing of our third-party technologies. Any weaknesses found are assessed and additional mitigation implemented where appropriate to ensure that the vulnerability is managed
- Our approach is aligned with the guidance provided within the international standard for application development, ISO27034
- The implementation is subject to regular independent tests via an IT Security Health CHECK test conducted by an NCSC-approved provider

## Cloud Security Principle 8 — Supply chain security

UKCloud Assured OFFICIAL Cloud and UKCloud Elevated OFFICIAL Cloud

- All UKCloud services are supported by a published Service Definition which states whether any third-party suppliers are directly involved in the provision of the service
- All key suppliers have signed a Control Affirmation document and are subject to regular audits to confirm their ability to support the security principles UKCloud has implemented
- Key suppliers are included within UKCloud's supplier assessment and internal audit programme, and have been independently assessed during Government Accreditor activities
- They are subject to regular, formal risk assessments as part of UKCloud's ISO27001–certified Information Security Management System

## Cloud Security Principle 9 — Secure consumer management

### UKCloud Assured OFFICIAL Cloud

- All users have a unique username, password and memorable word combination, with customisable expiry settings
- Customers can configure the Portal to require two-factor authentication
- UKCloud has also implemented Role Based Access Control (RBAC), allowing customers to control the level of access which their individual users have
- Customers can configure the Portal to allow connections for specified source IP addresses only
- This approach has been independently validated via NCSC design review, CHECK tests and ongoing accreditation activities.

### UKCloud Elevated OFFICIAL Cloud

- All users have a unique username, password and memorable word combination, with customisable expiry settings. Additionally, remote administrators are required to use a two-factor authentication system
- UKCloud has implemented Role Based Access Control (RBAC) allowing customers to control the level of access which their individual users have
- For additional security, connections are available only via an Assured WAN service, not directly from the internet.
- This approach has been independently validated via NCSC design review, CHECK tests and ongoing accreditation activities.

## Cloud Security Principle 10 — Identity and authentication

### UKCloud Assured OFFICIAL Cloud

- UKCloud creates the first administrator user account and communicates the credentials of this account using secure offline channels
- Customers can then create additional accounts using RBAC
- All accounts have a unique username, and all users are required to set a complex password in addition to a memorable word
- Consumers can configure source IP addresses to limit the networks that users can authenticate from (e.g. only authenticate from the office network and not home or public networks)
- All authentication requests are logged and analysed via the UKCloud GPG13-aligned protective monitoring service, which is operated 24/7
- This approach has previously been independently validated by NCSC Pan Government Accreditation, and continues to be regularly assessed by Government Accreditors

### UKCloud Elevated OFFICIAL Cloud

- UKCloud creates the first administrator user account and communicates the credentials of this account using secure offline channels
- Customers can then create additional accounts using RBAC
- All accounts have a unique username, and all users are required to set a complex password in addition to a memorable word. Additionally, remote administrators are required to use a two-factor authentication system
- Importantly, connections are only available via an Assured community WAN service, not directly from the internet, which reduces the opportunity for stolen credentials to be exploited
- All authentication requests are logged and analysed via the UKCloud GPG13-aligned protective monitoring service which is operated 24/7
- This approach has previously been independently validated by NCSC Pan Government Accreditation, and continues to be regularly assessed by Government Accreditors

## Cloud Security Principle 11 — External interface

### UKCloud Assured OFFICIAL Cloud

- Resilient internet connectivity is provided via multiple independent ISP circuits delivered into separate data centres
- As standard, internet connectivity is further protected against large-scale volumetric DDoS attacks using specialised protective infrastructure and resources
- UKCloud provides secure, resilient connectivity to government community networks including PSN (Assured Service), N3/HSCN and Janet
- Internet traffic shaping is used to ensure fair-sharing and prevent "noisy neighbour" (i.e. enforce customer separation)
- UKCloud has implemented IDS to detect malicious traffic patterns (e.g. port scans or ICMP flood)
- UKCloud operates managed physical firewalls to restrict the attack surface of customer solutions

### UKCloud Elevated OFFICIAL Cloud

- UKCloud provides secure, resilient connectivity to government secure networks including PSN (Protected Service), RLI and legacy networks such as GSI
- There is no direct connectivity to the internet. Connectivity to the internet requires all traffic to first successfully land within the UKCloud Assured OFFICIAL Cloud before passing through the Cross-Domain Security Zone (where AV, content checks, etc. are performed) which allows only whitelist services into this platform
- As this UKCloud platform does not have direct internet connectivity, NCSC considers it preferable to platforms with direct internet connections for higher-risk applications

## Cloud Security Principle 12 — Secure service administration

### UKCloud Assured OFFICIAL Cloud

- All UKCloud end-user devices used for administration are managed, secured and operated in line with NCSC published good practice
- UKCloud uses assured components (e.g. CPA-approved disk encryption) and two-factor authentication
- Authorised operations staff manage the platform using corporate end-user devices connecting via secure bastion hosts
- This approach has previously been independently validated by NCSC Pan Government Accreditation, and continues to be regularly assessed by Government Accreditors

### UKCloud Elevated OFFICIAL Cloud

- All UKCloud end-user devices used for administration are managed, secured and operated in line with NCSC published good practice
- UKCloud uses assured components (e.g. CPA-approved disk encryption) and two-factor authentication.
- Authorised operations staff manage the platform using dedicated end-user devices used solely for service management
- This makes it more difficult for the management devices and segregated network to be compromised
- This approach has previously been independently validated by NCSC Pan Government Accreditation, and continues to be regularly assessed by Government Accreditors
- This approach has previously been independently validated by NCSC Pan Government Accreditation, and continues to be regularly assessed by Government Accreditors

## Cloud Security Principle 13 — Audit information provision to consumers

UKCloud Assured OFFICIAL Cloud and UKCloud Elevated OFFICIAL Cloud

- UKCloud customers have access to a wide variety of management and log information using the secure UKCloud Portal
- UKCloud can offer customers limited audit information relating to their individual services upon receipt of a formal request for this information
- Due to the multi-tenant nature of our platform, we are required to sanitise the data before providing it to customers to ensure clear segregation of data relating to different customers
- This approach has previously been independently validated by NCSC Pan Government Accreditation, and continues to be regularly assessed by Government Accreditors

## Cloud Security Principle 14 — Secure use of the service by the consumer

UKCloud Assured OFFICIAL Cloud and UKCloud Elevated OFFICIAL Cloud

- UKCloud supports, enables and helps customers use its services securely through a combination of controls described across the other 13 principles. These include strong authentication, encryption, connectivity to government community networks and documented operational security (e.g. how to raise changes and incidents)
- UKCloud also provides white papers, blueprints, guides and other collateral, and training and support, to advise its customers on how to work securely
- NCSC's "Cloud Security Guidance: IaaS Consumer Guide" provides detailed guidance on how to work securely in the cloud.
- UKCloud helps its customers interpret and implement this NCSC guidance, supported by its experienced team of cloud architects