UKCLOUD SECURITY IMPLEMENTATIONS FOR THE HEALTH AND SOCIAL CARE SECURITY GOOD PRACTICE GUIDE

OPEN

ukcloud health

UKC-GEN-913

BACKGROUND

The Health and Social Care Cloud Security – Good Practice Guide (GPG) was created by the Department of Health and Social Care, NHS England, NHS Digital and NHS Improvement in 2018. It provides advice and guidance to NHS and social care organisations so that they can safely locate health and care data, including confidential patient information, in the public cloud.

The GPG uses the NCSC 14 Cloud Security Principles as a basis for its guidance, and this article details how UKCloud, as a supplier, has implemented each of the GPG recommendations.

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's full range of cloud services are regularly accredited or validated by many public sector organisations.

Please note that, whilst this article highlights UKCloud's obligations and responses, as the customer, you need to ensure you identify your obligations for adhering to the guidelines.

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

CLOUD SECURITY PRINCIPLE ONE: DATA IN TRANSIT PROTECTION

UKCloud Assured OFFICIAL Cloud

- TLS- (version 1.2) or SSL-encrypted sessions protect UKCloud services including access to the UKCloud Portal.
- Native internet connectivity is provided; customers can deploy their own VPN (for example, commercial grade), SSL/TLS or similar to protect their application over the internet.
- Customers can also connect via trusted networks (for example, PSN, HSCN, Janet).
- Traffic between UKCloud's data centres is protected using dedicated fibre circuits.
- Secure API proxy service protects exposed vendor APIs.
- Every aspect of our platform and the cloud services we provide are subject to regular, independent validation against ISO9001, ISO20000, ISO27001, ISO27017 and ISO27018.

UKCloud Elevated OFFICIAL Cloud

- TLS- (version 1.2) or SSL-encrypted sessions protect UKCloud services including 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 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 dedicated fibre circuits.
- Secure API proxy service protects exposed vendor APIs.
- Every aspect of our platform and the cloud services we provide are subject to regular, independent validation against ISO9001, ISO20000, ISO27001, ISO27017 and ISO27018.

CLOUD SECURITY PRINCIPLE TWO: ASSET PROTECTION AND RESILIENCE

UKCloud Assured OFFICIAL Cloud and Elevated OFFICIAL Cloud

- **2.1 Physical location and legal jurisdiction**
  - UKCloud services are hosted in multiple UK Ark data centres, adjacent to our UK operations centres, and separated by more than 100 km for excellent geo-resilience whilst maintaining UK sovereignty. 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 2018 and the EU General Data Protection Regulation 2016/679 (GDPR).
- **2.2 Data centre security**
  - All UKCloud data centres are subject to regular rigorous inspections and independent validation of their security controls (for example, physical perimeter, manned guarding, CCTV and access control systems) by NCSC and other Government Accreditors.
- **2.3 Data at rest protection**
  - The data centre infrastructure and facilities are regularly assessed and approved for all levels of information classification.
  - The UKCloud private cloud services can be supported by encryption facilities to ensure data is stored in an encrypted form, and this option is on the long-term roadmap for the UKCloud multi-tenant services. Customers requiring encrypted data at rest can either implement their own solution within their isolated multi-tenant environments or use the private cloud service. This encryption is verified in our auditing process for ISO27001.
- **2.4 Data sanitisation**
  - 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.

CLOUD SECURITY PRINCIPLE TWO: ASSET PROTECTION AND RESILIENCE

UKCloud Assured OFFICIAL Cloud and Elevated OFFICIAL Cloud

- **2.5 Equipment disposal**
  - UKCloud holds ISO27001 certification, and operates a Data Destruction Policy, which ensures that storage media that has contained customer data is securely stored in a media safe pending its secure sanitisation or physical destruction (for example, via assured components such as Blancco or Tabernus).
- **2.6 Physical resilience and availability**
  - 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 Ark 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.
  - Each service has a credit-backed SLA with strong reporting and remediation process. In order to assist customers in creating highly resilient workloads, UKCloud operates in two UK locations over four data centres, with at least eight availability regions containing multiple availability zones.

CLOUD SECURITY PRINCIPLE THREE: SEPARATION BETWEEN USERS

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 hypervisor technology such as VMware vSphere, Microsoft Azure and Red Hat OpenStack, 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 a NCSC-approved CHECK test provider, which supports the independent assurance of this platform.
- UKCloud holds and maintains certification to ISO27017, which was audited and checked by a UKAS-accredited audit body, as well as certification for Cyber Essentials Plus.

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 that further isolates customers from each other.
- Separation is further enhanced via assured components (for example, 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 a NCSC-approved CHECK provider, which supports the independent assurance of this platform.
- UKCloud holds and maintains certification to ISO27017, which was audited and checked by a UKAS-accredited audit body, as well as certification for Cyber Essentials Plus.

CLOUD SECURITY PRINCIPLE FOUR: GOVERNMENT FRAMEWORK

UKCloud Assured OFFICIAL Cloud and 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, ISO27017 and ISO27018 as well as other relevant international standards, which are audited by a UKAS-accredited audit body.
- 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.

CLOUD SECURITY PRINCIPLE FIVE: OPERATIONAL SECURITY

UKCloud Assured OFFICIAL Cloud and Elevated OFFICIAL Cloud

- These aspects have previously been independently validated by NCSC Pan Government Accreditation, and continue to be regularly assessed by Government Accreditors.
- UKCloud has ongoing PSN accreditation.
- **5.1 Configuration and change**
  - UKCloud's operational security activities are regularly assessed and independently validated under ISO27001 by a UKAS-accredited audit body and multiple Government Accreditors.
- **5.2 Vulnerability management**
  - UKCloud's operational security activities are regularly assessed and independently validated under ISO27001 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.
  - Internal processes and policies ensure that identified vulnerabilities should be mitigated within 24 hours for 'critical' vulnerabilities, within 2 weeks for 'important' vulnerabilities and within 8 weeks for 'other' vulnerabilities.

CLOUD SECURITY PRINCIPLE FIVE: OPERATIONAL SECURITY

UKCloud Assured OFFICIAL Cloud and Elevated OFFICIAL Cloud

- **5.3 Protective monitoring**
  - UKCloud's operational security activities are regularly assessed and independently validated under ISO27001 by a UKAS-accredited audit body and multiple Government Accreditors.
  - UKCloud conducts 24/7 protective monitoring to identify any suspicious activity, which is monitored and actioned by our 24/7 Cloud Operations team.
- **5.4 Incident management**
  - UKCloud's operational security activities are regularly assessed and independently validated under ISO27001 by a UKAS-accredited audit body and multiple Government Accreditors.
  - UKCloud have a regularly assessed and updated set of incident management processes used in the case of a security incident.
  - Service users are informed of any security incident that affects their environment or workloads.
  - UKCloud notifies security incidents to statutory organisations, such as NCSC 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 SIX: PERSONNEL SECURITY

UKCloud Assured OFFICIAL Cloud and 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 a minimum of Government Security Check (SC) level clearance, as well as NPPV (Non-Police Personnel Vetting) at Level 3 for working with police organisations. Many personnel additionally have Developed Vetting (DV) level clearance.
- These requirements exceed the requirements of BS7858:2012.
- All employees have signed the Official Secrets Act, are formally onboarded into operational environments and benefit from regular information security education and training. They also understand the robust framework of protective monitoring that records and analyses their individual activities.
- These aspects have previously been independently validated by NCSC Pan Government Accreditation and continue to be regularly assessed by Government Accreditors.

CLOUD SECURITY PRINCIPLE SEVEN: SECURE DEVELOPMENT

UKCloud Assured OFFICIAL Cloud and Elevated OFFICIAL Cloud

- UKCloud follows an agile development methodology, which allows it to adapt quickly 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 a NCSC-approved provider.

CLOUD SECURITY PRINCIPLE EIGHT: SUPPLY CHAIN MANAGEMENT

UKCloud Assured OFFICIAL Cloud and Elevated OFFICIAL Cloud

- All UKCloud services are supported by a published Service Definition that states whether any third-party suppliers are directly involved in the provision of the service.
- All key suppliers are subject to regular audits to confirm their ability to support the security principles and requirements UKCloud has implemented.
- They are subject to regular, formal risk assessments as part of UKCloud's Quality Management System (certified to ISO9001), IT Service Management Systems (certified to ISO20000) and Information Security Management System (certified to ISO27001)

CLOUD SECURITY PRINCIPLE NINE: SECURE USER MANAGEMENT

UKCloud Assured OFFICIAL Cloud

- **9.1 Authentication of [admin] users to management interfaces and support channels**
  - 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.
  - All access attempts are logged and can be reported on if required.
  - Access attempts, access security and logs are reviewed at regular intervals, during CHECK tests and ongoing accreditation activities.
- **9.2 Separation and access control within management interfaces**
  - UKCloud has also implemented Role Based Access Control (RBAC), enabling customers to control the level of access that 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

- **9.1 Authentication of [admin] users to management interfaces and support channels**
  - 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.
  - All access attempts are logged and can be reported on if required.
  - Access attempts, access security and logs are reviewed at regular intervals, during CHECK tests and ongoing accreditation activities.
  - Customers are recommended to log management and support requests via the UKCloud web portal but can also do so via email and telephone.
- **9.2 Separation and access control within management interfaces**
- UKCloud has implemented Role Based Access Control (RBAC) enabling 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 TEN: 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 (for example, only authenticate from their 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 ELEVEN: EXTERNAL INTERFACE PROTECTION

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 HSCN and Janet.
- Internet traffic shaping is used to ensure fair-sharing and prevent “noisy neighbour” (that is, enforce customer separation).
- UKCloud has implemented IDS to detect malicious traffic patterns (for example, 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, RLI and legacy networks such as GSI.
- There’s 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 and so on are performed), which allows only permissible services into this security domain.
- As this UKCloud security domain does not have direct internet connectivity, NCSC considers it preferable to security domains with direct internet connections for higher-risk applications.

CLOUD SECURITY PRINCIPLE TWELVE: 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 (for example, CPA-approved disk encryption) and two-factor authentication.
- Authorised operations staff manage the platform using corporate end-user devices connecting via secure bastion hosts.
- Comprehensive alert monitoring and event management tool set that will alert the 24/7 Cloud Operations team of any irregularities. These are then investigated, triaged and resolved immediately.
- Access to administration and management accounts and activities are limited to authorised personnel only, who switch between login accounts for other non-administration activities.
- 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 (for example, 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.
- Comprehensive alert monitoring and event management tool set that will alert the 24/7 Cloud Operations team of any irregularities. These are then investigated, triaged and resolved immediately.
- Access to administration and management accounts and activities are limited to authorised personnel only, who switch between login accounts for other non-administration activities.
- This approach has previously been independently validated by NCSC Pan Government Accreditation and continues to be regularly assessed by Government Accreditors.

CLOUD SECURITY PRINCIPLE THIRTEEN: AUDIT INFORMATION FOR USERS

UKCloud Assured OFFICIAL Cloud and Elevated OFFICIAL Cloud

- All activities on the platform are logged in real-time and available for review by authorised UKCloud administration users.
- UKCloud customers have access to a wide variety of management and log information using the secure UKCloud Portal or contacting their dedicated Service Delivery Manager.
- UKCloud can offer customers limited audit information relating to their individual services upon receipt of a formal request for this information.
- A secure facility is available to forward/export logs from the cloud platform to specified authorised users.
- Due to the multi-tenant nature of our platform, we're 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 FOURTEEN: SECURE USE OF THE SERVICE

UKCloud Assured OFFICIAL Cloud and Elevated OFFICIAL Cloud

- Customers create virtual machines using a set of prebuilt, tested and secure operating system images from the UKCloud Portal.
- Comprehensive alert monitoring and event management tool set that will alert the 24/7 Cloud Operations team of any irregularities. These are then investigated, triaged and resolved immediately.
- 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 (for example, 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 manage and work securely.
- NCSC's "Cloud Security Guidance" 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.