What is the Minimum Cyber Security Standard?

The Minimum Cyber Security Standard (MCSS) was published in June 2018 as the new minimum set of cyber security standards that the government expects its departments to adhere to, and exceed wherever possible. These standards also apply to any third-party supplier that provides services to a department and, as part of the process of following the MCSS, customers need to identify which standards are required to be evidenced by their supply chain.

Within the table below, we help customers understand the mature capabilities that can be recognised by using UKCloud Health. It is important to note that over time, these requirements are expected to evolve to continually 'raise the bar', address new threats or classes of vulnerabilities and incorporate the use of new Active Cyber Defence measures.

The standards relate to five key areas:

Standards 1, 2, 3, 4	**Identify**	• Departments shall put in place appropriate cyber security governance processes, and identify and catalogue sensitive information they hold. • Departments shall identify and catalogue the key operational services they provide. • The need for users to access sensitive information or key operational services shall be understood and continually managed.
Standards 5, 6, 7	**Protect**	• Access to sensitive information and key operational services shall only be provided to identified, authenticated and authorised users or systems. • Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities. • Highly privileged accounts should not be vulnerable to common cyber-attacks.
Standard 8	**Detect**	• Departments shall take steps to detect common cyberattacks including monitoring systems that evolve with the Department's business and technology changes, as well as changes in threats.
Standard 9	**Respond**	• Departments shall have a defined, planned and tested response to cyber security incidents that impact sensitive information or key operational services.
Standard 10	**Recover**	• Departments shall have well defined and tested processes in place to ensure the continuity of key operational services in the event of failure or compromise.

How should you be responding to the Minimum Cyber Security Standard?

UKCloud Health has developed mature capabilities with its comprehensive framework addressing information security, data protection and governance. Alongside the requirements within, further information is available in our responses to NHS digital, data and technology standards framework and the Data Security Protection Toolkit sections of this web page.

Standard	Customer responsibilities	How UKCloud Health can assist you	More information
1. Cyber security governance	Customers need to be able to demonstrate clear responsibilities and accountabilities, effective policies and processes, risk management, supply chain security and training and awareness.	When selecting a supplier, customers can be assured that UKCloud meets the requirements set out in the MCSS as detailed in the information in this table. We have significant experience in demonstrating compliance with a wide variety of standards and frameworks and will be able to provide the assurance evidence to support or reinforce your own department's position.	UKCloud's comprehensive G-Cloud Evidence Pack containing assurance information is available on request. UKCloud's own Data Security and Protection Toolkit (DSPT) is available on request. A review of the "Minimum Cyber Security Standard", blog written by UKCloud's Director of Compliance & Information Assurance. The highest standards for the UK Public Sector page on our website explains our approach and shows adherence to compliance frameworks. System Interconnect Security Policy (SISP) page on our website provides an overview of the SISP and explains the respective roles and responsibilities as the customer and

			the cloud service provider (UKCloud). We comply with the following ISO standards: • Information Security Management (ISO27001) • Security Controls for Cloud Services (ISO27017) • Personal Data in the Cloud Security (ISO27018)
2. Sensitive Information	Customers are required to have a full understanding of sensitive information assets, why and where they are being processed and stored, and the impact if any of them were to be breached or compromised.	UKCloud is fully aware that the data sets of health care customers are likely to contain sensitive information. As such, and as detailed elsewhere in this table, we provide a range of controls and functions to ensure that customer's sensitive information is securely processed, stored and managed at all times. The UKCloud platforms is subject to constant protective monitoring (which aligns with GPG13) and our 24/7 Network Operations Centre /Security Operations Centre capability provides near real time updates to customers.	UKCloud's comprehensive G-Cloud Evidence Pack containing assurance information is available on request. Monitoring the UKCloud platform - Knowledge Centre article, provides information on how we monitor our platform, including our security incident monitoring system that scans for potential security incidents 24 hours a day.

3. Operational service	Customers must have the details of key operational services being provided, knowledge of technology and other dependencies which they rely upon, and the impact of unavailability. Customers have a responsibility to understand the availability requirements of their data and systems and to ensure that they select an appropriate level of cloud service resilience to meet these objectives.	To help our customers understand the nature and suitability of our cloud services we provide comprehensive Service Definitions. If required for assurance purposes, we can also provide RMADS and Residual Risk Statements for each cloud service. We also have a comprehensive Knowledge Centre, containing articles and guidance on all our services. Our platform enables customers to implement resilient solutions depending on the priority of the service. If a particular solution requires absolute uptime, customers can design for resilience and high availability by utilising UKCloud's multiple sites (each with government network connectivity, including HSCN and PSN), which provide multiple instances of the same service to avoid downtime in the unlikely event of service failure in one location. In addition, customers can call on our free of charge team of Cloud Architects, who can help design the right solution depending on requirements and objectives. Status page To let customers, know of any updates to UKCloud services including new releases, planned maintenance and incidents	UKCloud Knowledge Centre – provides technical documentation on UKCloud's products and services. UKCloud Service Definitions – provides customers with a high-level introduction to the service outlining what it is, why the customer would choose this service and links to the supporting materials on the KC. Sites, Regions and Zones – Knowledge Centre article, which explains how customers can design applications that are highly resilient. UKCloud's comprehensive G-Cloud Evidence Pack containing assurance information is available on request.

4. User and access management	Customers are required to ensure that their users have only the minimum level of access to systems and information which are required for them to undertake their authorised duties. All such access should be monitored and logged and subject to regular review.	The UKCloud Portal enables its customers to determine the level of access and privileges that their users have within the virtual environment. The System Administrator has the authority to remove users using the self-service UKCloud Portal if they have left the company or no longer need access. Only security cleared personnel can access the underlying UKCloud platform in strict accordance with Role Based Access Control (RBAC). Such access is only authorised for valid business purposes, is subject to protective monitoring and logging and is regularly reviewed for compliance. By default, UKCloud personnel cannot access its cloud customers virtual environments.	We comply with the following ISO standard: • Information Security Management (ISO27001) UKCloud's comprehensive G-Cloud Evidence Pack containing assurance information is available on request. Getting Started Guide for the UKCloud Portal - Knowledge Centre article, which provides an overview of what customers can do in the Portal. Monitoring the UKCloud platform - Knowledge Centre article, provides information on how we monitor our platform, including our security incident monitoring system that scans for potential security incidents 24 hours a day. Portal user access - Knowledge Centre article, which explains the facilities available on the UKCloud Portal to manage user access.
5. Protecting access	Customers need to ensure that only authorised and known users can access sensitive data and	The UKCloud Portal, which provides access to UKCloud's services, is restricted to registered customer user accounts. The	UKCloud's comprehensive G-Cloud Evidence Pack containing assurance information is available on request.

	associated systems, and that appropriate access control, authentication and monitoring mechanisms are in place. It is recommended that customers review log files regularly and address any suspicious events.	permissions for each user must be set by an authorised customer administrator within the UKCloud Portal. UKCloud provides authentication mechanisms to its customers, which include: • Memorable words • 2FA (two-factor authentication): users may only login with a correct 2FA response • IP address restriction: users may only login to the UKCloud Portal from a pre-registered IP address.	2-Factor authentication – Knowledge Centre article, which provides a detailed overview of the security processes taken to access the UKCloud Portal. Portal permissions – Knowledge Centre article, which provides a detailed overview of the permissions page that only system administrators can access to set the account users' permissions.
6. Vulnerability management	Customers will need to demonstrate that they are effectively protecting enterprise technology, end-user devices, digital services and email communications through effective organisational and technical controls. This includes the identification, assessment and application of patches, upgrades and other updates to effectively manage all applicable cyber threats and vulnerabilities.	To ensure customers meet this standard, UKCloud's services can be accessed using properly managed corporate/enterprise devices only. The use of such devices must comply with all applicable controls specified within the UKCloud SISP (System Interconnect Security Policy), including asset management, device configuration, acceptable use, security incident reporting, and so on. The UKCloud platform is subject to constant monitoring such that all patches, upgrades and other updates are assessed, implemented and managed in a timely manner.	UKCloud's comprehensive G-Cloud Evidence Pack containing assurance information is available on request. System Interconnect Security Policy (SISP) page on our website provides an overview of the SISP and explains the respective roles and responsibilities as the customer and the cloud service provider (UKCloud). Status Page - To let customers, know of any updates to UKCloud services including new releases, planned maintenance and incidents.

7. Protecting privileged accounts	Customers will need to demonstrate that privileged accounts are only used for authorised administrative purposes and are not used for daily tasks. Their use should be protected by multi-factor authentication and complex passwords and be subject to protective monitoring.	Internally, UKCloud's Access Control Policy places specific responsibilities on UKCloud administrative accounts, which are privileged and not to be used routinely for normal support or development tasks. Super user accounts are tracked and recorded within the UKCloud protective monitoring system, clearly identifying the access and actions undertaken using the privileged account. The super user can then activate UKCloud's additional security features, such as 2FA, ensuring protection for all privileged accounts.	UKCloud's comprehensive G-Cloud Evidence Pack containing assurance information is available on request. Monitoring the UKCloud platform - Knowledge Centre article, provides information on how we monitor our platform, including our security incident monitoring system that scans for potential security incidents 24 hours a day. 2-Factor authentication – Knowledge Centre article, which provides a detailed overview of the security processes taken to access the UKCloud Portal. Portal permissions – Knowledge Centre article, which provides a detailed overview of the permissions page that only system administrators can access to set the account users' permissions.
8. Detecting common cyber-attacks	Customers are advised to undertake effective protective monitoring activities, including capturing and analysing events, which can then be assessed using threat intelligence sources such as CISP and CareCERT.	Monitoring and preventing common cyber-attacks is crucial to our operation. At UKCloud we offer DDoS mitigation and protective monitoring on customer's external endpoints as standard to monitor and detect threats. The UKCloud Customer platform is monitored by a GPG13-aligned protective	Visit this NCSC website to learn more about the Cyber Security Information Sharing Partnership (CISP). UKCloud receive and act upon regular CareCERT bulletins.

	It is also recommended that customers undertake periodic IT health checks to ensure that systems and applications are resilient against the current threat landscape.	monitoring system, operating at minimum DETER level, alongside perimeter packet analysis, a monthly external and general vulnerability scan and an annual NCSC-approved ITSHC CHECK Test. These measures applied build up defensive capabilities for customers through monitoring and detection. We are also part of the CISP platform and actively monitor and share threat information with customers. As part of our protective monitoring activities, we gather insight and knowledge from credible sources such as the CISP and CareCERT bulletins. Our technical personnel receive regular comprehensive training on the identification and management of cyber threats and vulnerabilities to ensure that the team are updated with the current threat landscape.	The benefits of protective monitoring This blog reviews the need for protective monitoring and the preventative measures that can be taken to avoid and resolve vulnerabilities. Application-tuned DDoS protection FAQ – Knowledge Centre article, which provides answers regarding what the service is and the effects of its use. Application-tuned DDoS protection service scope – Knowledge Centre article, which provides additional information regarding the optional Application-tuned DDoS protection service, used for protecting UKCloud services in addition to UKCloud's own standard DDoS protection.
9. Responding to cyber security incidents	Customers must implement effective plans to respond to incidents including defined responsibilities, communication plans, investigation and mitigation actions, incident reporting and plan testing.	Building upon the preparations outlined in standard 8 (above), UKCloud is committed to providing professional expert assistance to its customers to assist them to respond to cyber security incidents. This also includes cooperation in notifying the relevant authorities and cooperating in subsequent investigative and remedial activities.	UKCloud's comprehensive G-Cloud Evidence Pack containing assurance information is available on request.

10. Recovery of services	Customers need to ensure contingency plans are in place for unavailability of services or cyber security breaches and to ensure prompt restoration of normal service are well rehearsed, and that post incident reviews effectively remediate the cause to prevent recurrence.	As per standard 3, customers have the option of choosing UKCloud services and configuring them in a way that enables them to achieve their own resilience or availability requirements through native backup or restore solutions if workloads are on UKCloud. Customers also have the option of implementing their own business continuity solutions if desired. UKCloud's Zerto-powered services enable customers to recover from disaster scenarios such as cyber security breaches and provide test failover options to enable them to test how systems respond in the event of a disaster.	Sites, Regions and Zones – Knowledge Centre article, which explains how customers can design applications that are highly resilient. The Disaster Recover as a Service page on our website provides information on the options, features and benefits of DRaaS. This case study shows how Zerto technology can help restore services following cyber security breaches. UKCloud's comprehensive G-Cloud Evidence Pack containing assurance information is available on request.