UKAS CertCheck
Security Statement

UKAS is committed to using services that are secure and adopting effective security standards that align with industry best practices in the areas of security and service management. This document outlines the steps UKAS takes to ensure services and information remain secure, including specific measures related to the operation of UKAS CertCheck. UKAS's privacy notice contains further information on how we handle the data that we collect.

INFORMATION RELEVANT TO ALL UKAS SERVICES

INFORMATION SECURITY POLICY

UKAS maintains written policies which cover information security and define employee's responsibilities and acceptable use of information technology system resources. UKAS receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behaviour. These policies are periodically reviewed and updated as necessary.

Our policies cover a wide array of security related topics ranging from general standards with which every employee must comply, such as account, data, and physical security, to more specialised expectations covering internal applications and information systems.

PERSONNEL SECURITY

UKAS employees and contractors are required to conduct themselves in a manner consistent with the company's guidelines, including those regarding confidentiality, business ethics, appropriate usage, and professional standards. All newly hired employees or contractors are required to sign confidentiality agreements.

CRITICAL SUPPLIERS

All critical suppliers are reviewed and required to provide evidence of:

- ISO/IEC 27001 accredited certification from an accredited certification body if providing hosting, data, or information services.
- Any other accredited certification as applicable to the service they are providing
- Compliance to regulatory requirements including GDPR & PCI
- A security statement covering how they manage and maintain security, including prevention, detection, and ongoing maintenance of services.

For Cloud based services, we require all data to be hosted within the European Economic Area. Specifically:

- UKAS's current IT hosting partner is ISO/IEC 27001, ISO 14001, ISO/IEC 20000 and ISO 9001 certified by a UKAS accredited certification body and are a HM Government G-Cloud supplier. Within their datacentres they run Server monitoring tools across their hosted environment plus Advanced Threat Analytics (ATA) which monitors and reports on internal security events and external threats.
- All current cloud hosting providers use datacentres that have ISO/IEC 270001 certification from an accredited certification body, with data located in either the UK or the EU borders.
- UKAS engage an independent CREST, CHECK certified organisation to carry out full Penetration testing on an annual basis, covering all internal and external facing services and infrastructure, including 3rd party provided services and applications.
- Since March 2021 UKAS has held a Cyber Essentials Certificate of Assurance

INFRASTRUCTURE, HARDWARE & APPLICATIONS

- All servers, email services and end user devices run virus and malware software
- All servers and end user devices are security patched monthly with emergency patches applied when appropriate
- Applications running on servers and laptops are updated as appropriate
- End user devices are encrypted using bit-locker
- All laptops use secure VPN to connect to the UKAS Domain and cloud services
- Multi Factor Authentication is applied to cloud services
- Laptops can be remotely locked and removed from our domain
- Mobile phones are centrally managed and monitored and can be remotely wiped
- Cloud based applications are security checked prior to release
- WEEEE disposal and data deletion is undertaken by an organisation certified to ISO/IEC 27001, ISO 14001, ISO 22301 and ISO 9001.

ADDITIONAL INFORMATION SPECIFIC TO UKAS CERTCHECK

ORGANISATIONAL SECURITY

Information security roles and responsibilities are defined within UKAS CertCheck. Our specialist IT infrastructure and support partners for UKAS CertCheck provide expertise and support on information security, security auditing and compliance. Our partners receive and review information system security notifications on a regular basis and highlight security alerts and advisory information to UKAS CertCheck on a routine basis after assessing the risk and impact as appropriate.

UKAS CertCheck follows the Information Security frameworks laid out in ISO/IEC 27001 and ISO/IEC 27701.

DATA CENTRES

UKAS CertCheck is hosted on Amazon Web services (AWS), who hold accredited certification to ISO/IEC 27001, to provide data centres. AWS have policies, procedures,

and infrastructure to handle both physical security of its data centres as well as the environment from which the data centres operate.

The UKAS CertCheck systems and infrastructure are hosted in AWS data centres that are geographically dispersed within the UK to provide high availability and redundancy. You can find more information on AWS security here.

CHANGE MANAGEMENT

A change management process is maintained for UKAS CertCheck to ensure that all changes made are applied in a controlled manner. Changes to systems, network devices, and other system components, and physical and environment changes are monitored and controlled through a formal change control process. Changes are reviewed, approved, tested, and monitored post-implementation to ensure that the expected changes are operating as intended.

AUDITING AND LOGGING

Audit logs are maintained by our specialist IT infrastructure and support partners for UKAS CertCheck. These logs provide an account of which personnel have accessed which systems. Access to our auditing and logging tool is controlled by limiting access to authorised individuals. Security events are logged, monitored, and addressed. Network components, workstations, applications, and any monitoring tools are enabled to monitor user activity.

ANTIVIRUS AND MALWARE PROTECTION

Antivirus and malicious code protection are centrally managed and configured to retrieve the updated signatures and definitions available. Malicious code protection policies automatically apply updates to these protection mechanisms. Anti-virus tools are configured to run scans, virus detection, real-time file write activity and signature file updates.

SYSTEM BACKUPS

UKAS CertCheck has backup standards and guidelines and associated procedures for performing backup and restoration of data in a scheduled and timely manner. Controls are established to help safeguard backed up data. We also work to ensure that customer data is securely transferred or transported to and from backup locations. Periodic tests are conducted to test whether data can be safely recovered from backup devices.

NETWORK SECURITY

UKAS CertCheck's infrastructure servers reside behind high-availability firewalls and are monitored for the detection and prevention of various network security threats. Firewalls are utilised to help restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need.
UKAS CertCheck maintains separate development and production environments, firewalls provide adequate network segmentation.

Automated tools operated by Amazon web services (AWS) are deployed within the network and the data centre to support near-real-time analysis of events to support of detection of system-level attacks. You can find more information on AWS security here.

VULNERABILITY MANAGEMENT

Security assessments are done to identify vulnerabilities. Each vulnerability is reviewed to determine if it is applicable, ranked based on risk, and assigned for remediation.

PATCH MANAGEMENT

Our specialist IT infrastructure and support partners strive to apply to UKAS CertCheck the latest security patches and updates to operating systems, applications, and network infrastructure to mitigate exposure to vulnerabilities. Patch management processes are in place to implement security patch updates as they are released by vendors. Patches are tested prior to being deployed into production.

SECURE NETWORK CONNECTIONS

HTTPS encryption is configured for UKAS CertCheck application access. This helps to ensure that user data in transit is safe, secure, and available only to intended recipients. The level of encryption is negotiated to either SSL or TLS encryption and is dependent on what the web browser can support.

ROLE BASED ACCESS

Role based access controls are implemented for access to UKAS CertCheck. Processes and procedures are in place to address the removal of users. Access control lists define the behaviour of any user within our information systems, and security policies limit them to authorised behaviours.

AUTHENTICATION AND AUTHORISATION

UKAS CertCheck requires that authorised users be provisioned with unique account IDs. The password policy enforces the use of complex passwords, which are deployed to protect against unauthorised use of passwords. Multi-Factor Authentication, Captcha Codes, IP Tracking and Blocking and Unique URLs are utilised to further protect against unauthorised access to or misuse of the data or information contained in UKAS CertCheck.

DATA PROTECTION

UKAS CertCheck applies a common set of personal data management principles to data that we may process, handle, and store. Personal data is protected using appropriate physical, technical, and organisational security measures. Any non-public information UKAS CertCheck may process, handle or store is encrypted at rest and in transit. UKAS CertCheck only processes personal information in a way that is compatible with and relevant for the purpose for which it was collected or authorised in accordance with our privacy policy. We take all reasonable steps to protect information we receive from our users from loss, misuse or unauthorised access, disclosure and/or alteration.

UKAS CertCheck additionally utilises physical measures to protect data or information in UKAS CertCheck from being ‘mined’. Physical Measures used to protect data from mining include: Limits on data displayed on screen whilst searching, limits on numbers of hits returned on searches, search only from Certificate number or part of organisation name and inability to generate lists of data.