ArcGIS Online Compliance with NCSC Cloud Security Principles

Document History

Version	Date	Reason for Issue
1.0	24 April 2020	Document released
1.1	20 January 2021	Minor updates
1.2	17 October 2022	Minor updates
1.3	26 May 2023	Minor updates

Contents

Introduction

This document describes Esri UK's understanding of ArcGIS Online's compliance with the 14 NCSC cloud principles, based on customer data being stored within it. It was last updated in May 2023.

Compliance

Principle 1: Data in transit protection

Data in transit between the consumer's end user device, other services and ArcGIS Online is sent over the internet and encrypted using HTTPS TLS 1.2.

Data in transit within the service is protected using Interconnection Service Agreements (ISA) established between backend systems, specifying security integrity requirements.

Principle 2: Asset protection and resilience

Physical Location

EU hosting option

All ArcGIS Online customer data resides in EU countries within the confines of the Amazon Web Service EU-West-1 (Ireland) region with failover to EU-Central-1 (Germany) and Microsoft Azure North Europe (Ireland) region with failover in West Europe (Netherlands) ArcGIS Online customers will be notified if Esri proposes storing any of their data outside of these regions. Customer metadata (email addresses, logins etc.) remains on US soil.

US hosting option

All ArcGIS Online customer data resides on United States soil within the confines of the Amazon Web Service US Regions (East, West) and Microsoft Azure US Regions (South Central, East, West). ArcGIS Online customers will be notified if Esri proposes storing any of their data outside of the US.

All

The legal jurisdiction of the service provider is the United States of America.

Esri (UK) Ltd is registered with the following data protection authority:

The Information Commissioner's Office (ICO)
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 0303 123 1113 F. 01625 524510
www.ico.org.uk

Registration reference:	Z9843569
Registration Start date:	4 April 2007
Registration Expiry date:	3 April 2024

Data Centre Security

ArcGIS Online utilizes the World-Class Cloud Infrastructure of Microsoft Azure and Amazon Web Services, both of which have completed the CSA questionnaires for their capabilities and may be downloaded from the CSA Registry located at: https://cloudsecurityalliance.org/star/#_registry.

ArcGIS Online cloud infrastructure providers publish independent auditor reports and certifications to provide customers with considerable information regarding the policies, processes and controls established and operated by them. ArcGIS Online cloud infrastructure providers are ISO27001 compliant.

Data at Rest Protection

ArcGIS Online is audited in accordance with FedRAMP Tailored Low requirements. ArcGIS Online encrypts all customer data at rest with AES 256-bit encryption.

Data Sanitisation

ArcGIS Online utilizes the World-Class Cloud Infrastructure of Microsoft Azure and Amazon Web Services, both of which have completed the CSA questionnaires for their capabilities and may be downloaded from the CSA Registry located at: https://cloudsecurityalliance.org/star/#_registry.

ArcGIS Online cloud infrastructure providers publish independent auditor reports and certifications to provide customers with considerable information regarding the policies, processes and controls established and operated by them. When a storage device has reached the end of its useful life, ArcGIS Online cloud infrastructure provider procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. The cloud infrastructure providers use the techniques detailed in DoD 5220.22M ("National Industrial Security Program Operation Manual") or NIST 800-88 ("Guidelines for Media Sanitization)" to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry standard practices.

Equipment Disposal

ArcGIS Online utilizes the World-Class Cloud Infrastructure of Microsoft Azure and Amazon Web Services, both of which have completed the CSA questionnaires for their capabilities and may be downloaded from the CSA Registry located at: https://cloudsecurityalliance.org/star/#_registry.

ArcGIS Online cloud infrastructure providers publish independent auditor reports and certifications to provide customers with considerable information regarding the policies, processes and controls established and operated by them. When a storage device has reached the end of its useful life, ArcGIS Online cloud infrastructure providers procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. The cloud infrastructure providers use the techniques detailed in DoD 5220.22M ("National Industrial Security Program Operation Manual") or NIST 800-88 ("Guidelines for Media Sanitization)" to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry standard practices.

Physical Resilience & Availability

Esri will use commercially reasonable efforts to make the service available with a Quarterly Uptime Percentage of 99.9% ("Service Commitment"). For any service quarter that the quarterly uptime percentage is less than this, customers will receive an SLA credit equivalent to the net Covered Downtime during the relevant service quarter in excess of the maximum Downtime permitted under the Service Commitment. Customers will receive 1 day of SLA Credit for every 24 hours (or fraction thereof) of covered Excess Downtime.

Amazon Web Services and Microsoft Azure public service level agreements are available for review through the respective service providers. Azure's main underlying network infrastructure is currently managed by Microsoft's Global Foundation Services (GFS). SLAs to service providers or equipment manufacturers are qualified by GFS's ISO 27001 certification. Microsoft Azure SLA information is available at http://www.windowsazure.com/en-us/support/legal/sla/. Amazon Web Services EC2 SLA information is available at: http://aws.amazon.com/ec2-sla/ and other AWS component SLA's are also available at this site.

The ArcGIS Online cloud infrastructure providers have business continuity policies and plans that are in alignment with ISO 27001 standards. ArcGIS Online has a contingency plan and utilizes redundant cloud infrastructure to minimize outages.

Historical evidence of the availability of the service is available at http://status.arcgis.com.

Principle 3: Separation Between Consumers

The service is Public Cloud. Details of the service are documented at http://doc.arcgis.com/en/arcgis-online/.

Physical and logical controls are implemented by cloud infrastructure providers and fully documented. ArcGIS Online feature service data is stored in separate database instances per organization. A separate Data Loss Prevention (DLP) solution has not been deployed for ArcGIS Online. It is recommended that customers do not allow public sharing from their ArcGIS Online organization unless required. This can be configured in the security settings for organization.

The cloud infrastructure providers utilize multiple separate network segments. This infrastructure provider segmentation helps to provide separation of critical, back-end servers and storage devices from the public-facing interfaces. Cloud infrastructure provider network segmentation aligns with ISO 27001 standards. Cloud infrastructure provider firewalls and host-based firewalls are utilized to separate various ArcGIS Online components.

Building and validating ArcGIS Online code against leading security industry standards such as OWASP is the foundation for building a robust offering. This is enforced within the continuous monitoring requirements of the ArcGIS Online FedRAMP authorization. ArcGIS Online is scanned at a minimum of every 30 days to ensure services are regularly validated against standards such as OWASP.

Principle 4: Governance Framework

The name and job title of the person in our organisation responsible for the security of the proposed service is Mark Wells, Chief Technology Officer, Esri UK. Esri Inc also have a dedicated security team, led by the Chief Product Security Office, Michael Young. ArcGIS Online complies with data protection and privacy laws generally applicable to Esri's provision of ArcGIS Online.

ArcGIS Online is compliant with FedRAMP Tailored Low requirements which is based on the NIST SP 800-53 control framework helping to ensure ArcGIS Online complies with applicable data protection and privacy laws. ArcGIS Online has an established process for identifying and implementing changes to services in response to changes in applicable statutes and regulations.

Third party risk assessments are performed at least annually, and a continuous monitoring plan is in place as specified by FedRAMP requirements for ArcGIS Online. Decisions to update policies and procedures are based on the risk assessment reports. Risk assessments are regularly reviewed based on periodicity and changes emerging to the risk landscape.

The ArcGIS Online Privacy Statement is certified compliant with independent, international, industry- accepted privacy standards including TRUSTe Certified Privacy Seal and EU Privacy Shield and is GDPR aligned. For more information see http://trust.arcgis.com.

ArcGIS Online provides customer remuneration for losses they may incur due to outages in alignment with ArcGIS Online Service Level Agreement available at: https://www.esri.com/content/dam/esrisites/en-us/media/legal/referenced-files/g-632-agol-service-level.pdf.

ArcGIS Online is audited in accordance with FedRAMP Tailored Low requirements. ArcGIS Online utilizes cloud infrastructure from MS Azure and Amazon Web Services. Each of the cloud infrastructure providers regularly audit their operations and can provide them under their own NDAs. ArcGIS Online utilizes third party auditors as part of FedRAMP Tailored Low compliance. Continuous monitoring includes vulnerability assessments and security control reviews. For security and operational reasons, Esri does not allow our customers to perform their own audits on ArcGIS Online as stated in the Terms of Service.

Principle 5: Operational Security

Configuration and change management

ArcGIS Online is audited annually by a third-party assessor to ensure its alignment with FedRAMP Tailored Low requirements. Esri maintains separate non-production systems for testing and validating new development and systems infrastructure capabilities as outlined in the internal ArcGIS Online Configuration Management Plan, aligning with FedRAMP requirements. ArcGIS Online conducts testing and validation prior to release in accordance with FedRAMP Tailored Low requirements. Cloud infrastructure providers ensure changes are tested in various test environments and signed off prior to deployment into production and ensuring alignment with the ISO 27001 standard.

Vulnerability Management

ArcGIS Online releases, which include patches and bug fixes, are performed quarterly. If security vulnerabilities are found or reported, they are assessed by security staff. Any vulnerabilities that have an assessed risk of high or critical are patched immediately outside of normal patching routines. Security patches are deployed monthly by default, however critical security patches are deployed within 7 days. As part of the FedRAMP accreditation requirements, ArcGIS Online is scanned at a minimum of every 30 days to ensure services are regularly validated against standards such as OWASP.

Protective Monitoring

A number of key security parameters are monitored to identify potentially malicious activity on the systems. Cloud infrastructure provider anti-virus controls align with ISO 27001 requirements.

Incident Management

Consumers report incidents and security concerns via the Esri UK support desk. We provide feedback on incidents at http://status.arcgis.com. Incident management processes are described within ArcGIS Online's Incident Response Plan documentation, aligning with FedRAMP requirements.

Principle 6: Personnel Security

All ArcGIS Online and cloud infrastructure provider employees are required to complete a standard background check as part of the hiring process. Background checks may include but are not limited to review of information relating to a candidate's education, employment and criminal history.

Principle 7: Secure Development

Esri utilizes the Building Security In Maturity Model (BSIMM) as the backbone to measure its efforts to immerse security throughout the development life cycle in the most effective manner for its products. Development is carried out in line with industry good practice regarding secure design, coding, testing and deployment. Configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment. Esri maintains separate development, staging and

production systems for testing and validating new development and systems infrastructure capabilities as outlined in the internal ArcGIS Online Configuration Management Plan, aligning with FedRAMP requirements.

Principle 8: Supply chain security

Cloud infrastructure provider access is only available on a need-to-know basis and managed by their ISO 27001 security controls. In alignment with ISO 27001 standards, cloud infrastructure provider hardware assets are assigned an owner, tracked and monitored by their personnel with inventory management tools. The cloud infrastructure procurement and supply chain team maintain relationships with all suppliers. Employees, contractors and third-party users are notified to destroy or return, as applicable, any physical materials that Esri has provided to them during the term of employment or the period of Contractor agreement and any electronic media must be removed from Contractor or third-party infrastructure. Esri periodically utilizes third party assessors for their products. ArcGIS Online utilizes cloud infrastructure from MS Azure and Amazon Web Services. Each of the cloud infrastructure providers regularly audit their operations and can provide them under their own NDAs.

Principle 9: Secure Consumer Management

Authentication of Consumers to Management Interfaces and Within Support Channels

Organizations should utilize ArcGIS Online Enterprise Logins to meet all of their organization's username and password management requirements and for adherence to FedRAMP and ISO 27001 security requirements. Further information concerning ArcGIS Online Enterprise Logins may be found at: http://resources.arcgis.com/en/help/arcgisonline/010q/010q000000vs000000.htm.

ArcGIS Online users can configure their Enterprise Logins to utilize their organization's two factor authentication solution which can align with requirements such as: HSPD-12, PIV and CAC. In addition, customers can choose to enable multi-factor authentication for their ArcGIS Organization independent of Enterprise Logins. For more information, see: https://doc.arcgis.com/en/arcgis-online/reference/multifactor.htm. Cloud infrastructure providers ensure two-factor authentication is utilized for their administrative operations.

If an Identity Provider (IdP) is not available ArcGIS Online enables administrators to implement a custom password policy for their ArcGIS Online organization. Other than User ID lockouts which are fixed settings, password policies can be customized to meet these requirements, or the specific requirements outlined in the customer's policies. For more info on setting a custom password policy, see: https://doc.arcgis.com/en/arcgisonline/administer/configure-security.htm

ArcGIS Online employees adhere to a rules of behaviour policy outlining user responsibilities. This includes guidance on safeguarding resources used to administer ArcGIS Online.

Separation and Access Control within Management Interfaces

ArcGIS Online is a multi-tenancy application. Administrators must log in to their organisational account within the service as described above. Once the administrator is authenticated, the service is responsible for ensuring only details relating to that organisation are shown.

A secure, role-based access control system is used for consumer administrators. Cloud infrastructure providers utilize segregation of duties for critical functional to minimize the risk of unintentional or unauthorized access or change to production systems.

Customers retain the ability to manage segregation of duties of their ArcGIS Online organization resources. The use of custom roles within ArcGIS Online enables permissions of specific user groups to be applied with much more granularity than the default roles of Administrator, Publisher and User. For additional information, see: http://doc.arcgis.com/en/arcgis-online/reference/roles.htm.

Principle 10: Identity and Authentication

Organizations should utilize ArcGIS Online Enterprise Logins to meet all of their organization's username and password management requirements and for adherence to FedRAMP and ISO 27001 security requirements. Further information concerning ArcGIS Online Enterprise Logins may be found at: http://resources.arcgis.com/en/help/arcgisonline/010q/010q000000vs000000.htm.

ArcGIS Online users can configure their Enterprise Logins to utilize their organization's two factor authentication solution which can align with requirements such as: HSPD-12, PIV and CAC. In addition, customers can choose to enable multi-factor authentication for their ArcGIS Organization independent of Enterprise Logins. For more information, see: https://doc.arcgis.com/en/arcgis-online/reference/multifactor.htm. Cloud infrastructure providers ensure two-factor authentication is utilized for their administrative operations.

If an Identity Provider (IdP) is not available ArcGIS Online enables administrators to implement a custom password policy for their ArcGIS Online organization. Other than User ID lockouts which are fixed settings, password policies can be customized to meet these requirements, or the specific requirements outlined in the customer's policies. For more info on setting a custom password policy, see: https://doc.arcgis.com/en/arcgisonline/administer/configure-security.htm

ArcGIS Online system administrator roles and responsibilities are documented within the internal ArcGIS Online System Security Plan. End-user roles and responsibilities are documented within the ArcGIS Online application documentation. Customers retain the ability to manage segregation of duties of their ArcGIS Online organization resources. The use of custom roles within ArcGIS Online enables permissions of specific user groups to be applied with much more granularity than the default roles of Administrator, Publisher and User. For additional information, see: http://doc.arcgis.com/en/arcgis-online/reference/roles.htm.

Principle 11: External Interface Protection

All service interfaces, except for service provider administration, are available over the Internet, encrypted using HTTPS TLS 1.2.

Cloud infrastructure provider network segmentation aligns with ISO 27001 standards. Cloud infrastructure provider firewalls and host-based firewalls are utilized to separate various ArcGIS Online components.

Esri publishes guidance to end users and consumer administrators on the safe use of the proposed service. Prior to granting access to ArcGIS Online services, customers are required to review and agree to the terms of use. The ArcGIS Online terms of use are available at: http://www.esri.com/legal/pdfs/mla_e204_e300/english.html/#Addendum_3. End user documentation is available at http://doc.arcgis.com/en/arcgis-online/ and http://trust.arcgis.com, including safe use of the service.

Principle 12: Secure Service Administration

Cloud infrastructure shared network access is strictly restricted to critical resources including services, hosts and network devices and must be explicitly approved.

Protection of wireless devices and ensuring encryption are part of regular network management security practices within Esri (includes monitoring). Cloud infrastructure providers manage equipment identification in alignment with the ISO 27001 standard. Cloud infrastructure provider personnel are required to adhere to applicable policies, which do not permit mobile computing devices to the production environment, unless those devices have been approved for use by cloud infrastructure management.

ArcGIS Online employees adhere to a rules of behaviour policy outlining user responsibilities. This includes guidance on safeguarding resources used to administer ArcGIS Online.

Direct Service Management is used as a Service Management Model.

Principle 13: Audit Information Provision to Consumers

Customers have access to a detailed audit log within ArcGIS Online known as the Organisational Activity Log. detailing activity within their organisational account. Information such as last login is also available to administrators.

Access to information systems audit tools is restricted to authorized personnel within ArcGIS Online.

Access to logs is restricted as defined by policy, and logs are reviewed on a regular basis in alignment with FedRAMP Tailored Low requirements. Audit logs are retained as defined by ArcGIS online retention policy which is in alignment with FedRAMP Tailored Low requirements.

All ArcGIS Online UK customers have a dedicated Esri UK Customer Success Manager whose job is to support customer's use of Esri technology. This includes supporting a security investigation which included ArcGIS Online in its scope. The Customer Success Manager will then use Esri UK Solution Architects and Support Channels to Esri Inc as necessary. Our procedure for handling security investigations from 3rd parties will depend on the nature of the 3rd party, the nature of the investigation and the jurisdiction that it takes place under.

Principle 14 Secure Use of the Service by the Consumer

All access to the service is via the Internet over HTTPS as described in other responses. However, access to customer data (stored in customer data centres) from the service

itself or from end-user devices to use within the service can be secured as a customer sees fit. For example, they can successfully use the service using URLs that are only accessible internally if all their users are using managed devices. Or they can use public URLs that resolve to servers in or through their perimeter network.

ArcGIS Online users can configure their Enterprise Logins to utilize their organization's two factor authentication solution which can align with requirements such as: HSPD-12, PIV and CAC. In addition, customers can choose to enable multi-factor authentication for their ArcGIS Organization independent of Enterprise Logins. For more information, see: https://doc.arcgis.com/en/arcgis-online/reference/multifactor.htm.

If an Identity Provider (IdP) is not available ArcGIS Online enables administrators to implement a custom password policy for their ArcGIS Online organization. Other than User ID lockouts which are fixed settings, password policies can be customized to meet these requirements, or the specific requirements outlined in the customer's policies. For more info on setting a custom password policy, see: https://doc.arcgis.com/en/arcgisonline/administer/configure-security.htm.

Access from a wireless network on a customer premise to the ArcGIS Online environment must be secured by the customer.

ArcGIS Online does not require installable mobile code such as MS ActiveX, Adobe Flash and MS Silverlight.

References

Reference Id	Name/URL	Version
1	ArcGIS Online Cloud Controls Matrix	July 2021
2	Information Commissioners Office Data Protection Public Register	May 2023
3	NCSC Cloud Security Guidance	May 2022

End of document