ArcGIS Online
Higher Education Information Security Council (HEISC) Higher Education Community Vendor Assessment Tool (HECVAT Lite) 3.04 July 2023

Attached are Esri's self-assessment answers to the Higher Education Information Security Council (HEISC) Higher Education Community Vendor Assessment Tool (HECVAT Lite) for ArcGIS Online. The questionnaire published by the HEISC, provides a comprehensive understanding of the security measures implemented by ArcGIS Online using the HECVAT Lite framework. Essential to higher education institutions, the HECVAT Lite helps to ensure strong information security and security control practices, updated security programs, and effective incident response plans. This is designed for IT professionals and administrators in higher education to assist institutions in making informed decisions in the use of ArcGIS Online securely and in compliance with their institution's policies.

The Higher Education Information Security Council (HEISC) is a collaborative body that supports higher education institutions as they improve information security governance, compliance, data protection, and privacy programs. The council, formed under EDUCAUSE, a nonprofit association that advances higher education using information technology, is dedicated to enhancing the state of information security and privacy across the higher education sector.

ArcGIS Online is audited annually by a 3rd party assessor to ensure alignment with its Federal Risk and Authorization Management Program (FedRAMP) Authority to Operate (ATO) by the United States Department of Interior. For more information concerning the security, privacy, and compliance of ArcGIS Online please see the ArcGIS Trust Center at: https://Trust.ArcGIS.com

ArcGIS Online utilizes the World-Class Cloud Infrastructure of Microsoft Azure and Amazon Web Services, both of which have completed HECVAT questionnaires for their capabilities and may be viewed at the Amazon Web Services and Microsoft Azure websites.

The latest version of the ArcGIS Online HECVAT Lite answers will be available at the following location until further notice:
https://downloads.esri.com/resources/enterprisegis/AGOL_HECVAT.pdf

For a more lightweight set of answers, a basic overview of ArcGIS Online security (2-page flyer) is available within the Trust Center documents. Some basic, recurring customer questions include:

- Where is my data hosted? Within AWS and MS Azure datacenters on US Soil by default, new organizations can choose to have their data stored in regions outside the US, such as the EU or AP Regions.
- Is my data encrypted at rest and in transit? Yes, organizations use HTTPS w/TLS 1.2 for in-transit and AES-256 at rest.
- Is my data backed up? Customers are responsible for backing up their datasets.
- Can I do security tests against ArcGIS Online? Yes, however a Security Assessment Agreement (SAA) must be completed first.
- Are my files scanned with Anti-virus? Yes – Files containing malicious code are rejected from upload.
- What privacy assurance is in place? ArcGIS Online is both GDPR and CCPA aligned.

For any questions/concerns/feedback please contact Esri's Software Security & Privacy Team at:
SoftwareSecurity@Esri.com

HECVAT - Lite | Vendor Response

Vendor Response

DATE-01	**Date**	*4/22/2023*

General Information

In order to protect the institution and its systems, vendors whose products and/or services will access and/or host institutional data must complete the Higher Education Community Vendor Assessment Toolkit. Throughout this tool, anywhere where the term data is used, this is an all-encompassing term including at least data and metadata. Answers will be reviewed by institution security analysts upon submittal. This process will assist the institution in preventing breaches of protected information and comply with institution policy, state, and federal law. This is intended for use by vendors participating in a Third Party Security Assessment and should be completed by a vendor.

GNRL-01	Vendor Name	Esri
GNRL-02	Product Name	ArcGIS Online
GNRL-03	Product Description	ArcGIS Online is a secured, reliable geographic information system (GIS) delivered using the software-as-a-service (SaaS) model.
GNRL-04	Web Link to Product Privacy Notice	https://www.vendor.domain/privacynotice
GNRL-05	Web Link to Accessibility Statement or VPAT	https://www.esri.com/content/dam/esrisites/en-us/media/legal/vpats/arcgis-online-march-2022-vpat.pdf
GNRL-06	Vendor Contact Name	Esri
GNRL-07	Vendor Contact Title	Software Security and Privacy Team
GNRL-08	Vendor Contact Email	Software_Security@esri.com
GNRL-09	Vendor Contact Phone Number	909-793-2853
GNRL-10	Vendor Accessibility Contact Name	Esri Accessibility Team
GNRL-11	Vendor Accessibility Contact Title	Esri Accessibility Team
GNRL-12	Vendor Accessibility Contact Email	EsriAccessibility@esri.com
GNRL-13	Vendor Accessibility Contact Phone Number	909-793-2853
GNRL-14	Vendor Hosting Regions	By default all ArcGIS Online customer data resides on United States soil within the confines of the Amazon Web Service US Regions
GNRL-15	Vendor Work Locations	Redlands, CA

Vendor Instructions

Step 1: Complete each section answering each set of questions in order from top to bottom; the built-in formatting logic relies on this order. **Step 2**: Submit the completed Higher Education Community Vendor Assessment Toolkit - Lite to the requesting institution.

Company Overview		Vendor Answers	Additional Information
COMP-01	Describe your organization's business background and ownership structure, including all parent and subsidiary relationships.	Private Geographic Information System (GIS) software vendor with global distributors	
COMP-02	Have you had an unplanned disruption to this product/service in the last 12 months?	No	See status.arcgis.com
COMP-03	Do you have a dedicated Information Security staff or office?	Yes	Esri's Software Security & Privacy team is dedicated to the security and privacy assurance of our products.
COMP-04	Do you have a dedicated Software and System Development team(s)? (e.g. Customer Support, Implementation, Product Management, etc.)	Yes	See Esri.com for company structure details.
COMP-05	Does your product process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act?	No	Datasets uploaded to ArcGIS Online are owned by the customer and they are responsible for classifying their dataset and handling accordingly. It is the Customer's sole responsibility to ensure that Customer Content is suitable for use with Online Services. ArcGIS Online has select HIPAA eligable services available as described within the ArcGIS Trust Center

COMP-06	Will data regulated by PCI DSS reside in the vended product?	No	Esri stores no payment instrument number information (e.g. credit card) within their systems for Products & Services. Esri utilizes a third party provider which has been audited by a Payment Card Industry Standard certified auditor to ensure your information remains secure. Payment information is transmitted directly to the provider via HTTPS for secure transmission so that payment data is never transmitted or stored by Esri Products & Services.
COMP-07	Use this area to share information about your environment that will assist those who are assessing your company data security program.	See the ArcGIS Trust Center for details about ArcGIS Online Security & Privacy	
Documentation		**Vendor Answers**	**Additional Information**
DOCU-01	Have you undergone a SSAE 18 / SOC 2 audit?	No	No plan for SSAE 16 as FedRAMP Tailored Low authorization in place is more comprehensive
DOCU-02	Have you completed the Cloud Security Alliance (CSA) CAIQ?	Yes	ArcGIS Online standards are based on FedRAMP Tailored Low requirements. Also, this Cloud Security Alliance (CSA) CAIQ for ArcGIS Online is available to customers and can be viewed here: https://downloads.esri.com/RESOURCES/ENTERPRISEGIS/AGOL_CSA_CAIQ.PDF
DOCU-03	Have you received the Cloud Security Alliance STAR certification?	No	Esri ArcGIS Online is STAR Level One since 8/19/2015. Current CAIQ can be viewed on our ArcGIS Trust Center: https://downloads.esri.com/RESOURCES/ENTERPRISEGIS/AGOL_CSA_CAIQ.PDF
DOCU-04	Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)	Yes	ArcGIS Online is FedRAMP authorized which is based on NIST security controls.
DOCU-05	Can the systems that hold the institution's data be compliant with NIST SP 800-171 and/or CMMC Level 3 standards?	Yes	ArcGIS Online is FedRAMP authorized which is based on NIST security controls. The offering is shifting from Tailored Low to Moderate in 2023. NIST 800-171 is a subset of FedRAMP Moderate security controls.
DOCU-06	Can you provide overall system and/or application architecture diagrams including a full description of the data flow for all components of the system?	Yes	Please review this online resource for more information: https://downloads.esri.com/resources/enterprisegis/ArcGIS_Online_Security.pdf
DOCU-07	Does your organization have a data privacy policy?	Yes	Esri's Privacy Statement and Products & Services Privacy Statement Supplement are available on our Trust Center: https://trust.arcgis.com/en/privacy/privacy-tab-intro.htm
DOCU-08	Do you have a documented, and currently implemented, employee onboarding and offboarding policy?	Yes	All employees must have a background check before being onboarded into ArcGIS Online - Employees access is removed same day as offboarding.
DOCU-09	Do you have a well documented Business Continuity Plan (BCP) that is tested annually?	Yes	ArcGIS Online has a full Continuity Plan designed in alignment with FedRAMP Tailored Low security control requirements. ArcGIS Online cloud Infrastructure providers ensure their business continuity plans align with ISO 27001 standards.
DOCU-10	Do you have a well documented Disaster Recovery Plan (DRP) that is tested annually?	Yes	The DRP is required for FedRAMP and assessed annually by a 3rd party.
DOCU-11	Do you have a documented change management process?	Yes	All changes to the ArcGIS Online infrastructure are tracked and recorded through the Change Management documented processes and Procedures, scheduled maintenance windows are published to the ArcGIS Online Status dashboard where any customer can subscribe to for updates at https://status.arcgis.com.
DOCU-12	Has a VPAT or ACR been created or updated for the product and version under consideration within the past year?	Yes	https://www.esri.com/en-us/legal/accessibility/conformance-reports
DOCU-13	Do you have documentation to support the accessibility features of your product?	Yes	Please review the following https://www.esri.com/en-us/accessibility/overview. This includes resources and conformance reports for our core products including ArcGIS Online.

IT Accessibility		Vendor Answers	Additional Information
ITAC-01	Has a third party expert conducted an accessibility audit of the most recent version of your product?	Yes	April 15, 2022 the product was tested by certified accessbility professionals and the Esri Accessbility Conformance Report can be viewed here: https://www.esri.com/content/dam/esrisites/en-us/media/legal/vpats/arcgis-online-march-2022-vpat.pdf
ITAC-02	Do you have a documented and implemented process for verifying accessibility conformance?	Yes	Please review the following https://www.esri.com/en-us/accessibility/overview. This includes resources and conformance reports for our core products including ArcGIS Online.
ITAC-03	Have you adopted a technical or legal accessibility standard of conformance for the product in question?	Yes	Please see the following link for details: https://www.esri.com/en-us/legal/accessibility/accessibility-overview
ITAC-04	Can you provide a current, detailed accessibility roadmap with delivery timelines?	Yes	For details to the latest approach to accessibility at Esri, please see the following page: https://www.esri.com/en-us/accessibility/overview
ITAC-05	Do you expect your staff to maintain a current skill set in IT accessibility?	Yes	Yes, Esri has a dedicated accessibility team who's effort is to achieve product accessibility for all begins with diligent research of evolving accessibility capabilities and continues with the development and incorporation of these capabilities into GIS functions across our product line.
ITAC-06	Do you have a documented and implemented process for reporting and tracking accessibility issues?	Yes	Our core product development teams conduct accessibility testing events and are provided with testing tools, resources and materials, and internal support from accessibility subject matter experts (SMEs) throughout the company.
ITAC-07	Do you have documented processes and procedures for implementing accessibility into your development lifecycle?	Yes	Esri recognizes the importance of adhering to accessibility guidelines and standards for all users of our products, including users with disabilities. We conduct Accessibility Conformance Reports (ACR®) for Esri products, solutions, and services. Each report describes the conformance level for accessibility features, assistive technologies, and evaluation methods used, with additional information about general product accessibility. We incorporate inclusive design principles throughout the creation of Esri core software, website, and design systems. Our ongoing mission is reflected in the usability of our products and solutions. 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. ArcGIS Online is FedRAMP Tailored Low authorized and therefore also aligns with NIST standards. Please see our Secure Development Lifecycle Overview on within the ArcGIS Trust Center documents https://trust.arcgis.com for more information.
ITAC-08	Can all functions of the application or service be performed using only the keyboard?	Yes	Please see the following documentation for details: https://www.esri.com/content/dam/esrisites/en-us/media/legal/vpats/arcgis-online-march-2022-vpat.pdf
ITAC-09	Does your product rely on activating a special 'accessibility mode,' a 'lite version' or accessing an alternate interface for accessibility purposes?	No	

Application/Service Security		Vendor Answers	Additional Information
HLAP-01	Are access controls for institutional accounts based on structured rules, such as role-based access control (RBAC), attribute-based access control (ABAC) or policy-based access control (PBAC)?	Yes	ArcGIS Online relies on the Role Based Access Control (RBAC) model. All users in solution need to have a role for which they are granted access to.

HLAP-02	Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?	Yes	ArcGIS Online relies on the Role Based Access Control (RBAC) model. All users in solution need to have a role for which they are granted access to.
HLAP-03	Do you have a documented and currently implemented strategy for securing employee workstations when they work remotely? (i.e. not in a trusted computing environment)	Yes	Yes, there is an employee work from home guide.
HLAP-04	Does the system provide data input validation and error messages?	Yes	See online help here:https://developers.arcgis.com/net/reference/platform-error-codes/
HLAP-05	Are you using a web application firewall (WAF)?	Yes	
HLAP-06	Do you have a process and implemented procedures for managing your software supply chain (e.g. libraries, repositories, frameworks, etc)	Yes	See Esri Software Security Overview document within the ArcGIS Trust Center.
Authentication, Authorization, and Accounting		**Vendor Answers**	**Additional Information**
HLAA-01	Does your solution support single sign-on (SSO) protocols for user and administrator authentication?	Yes	Organizations can choose to utilize ArcGIS Online Organization Specific Logins (Esri's version of SSO - using the SAML standard) to meet all of their organization's username and password management requirements and for adherence to FedRAMP and ISO 27001 security requirements.
HLAA-02	Does your organization participate in InCommon or another eduGAIN affiliated trust federation?	Yes	ArcGIS Online supports federation of identity providers as documented here: https://doc.arcgis.com/en/arcgis-online/administer/saml-logins.htm
HLAA-03	Does your application support integration with other authentication and authorization systems?	Yes	Customers are responsible for managing authentication & access to their the ArcGIS Online application using a SAML 2.0 compliant Identity Provider (IdP).
HLAA-04	Does your solution support any of the following Web SSO standards? [e.g., SAML2 (with redirect flow), OIDC, CAS, or other]	Yes	SAML 2.0, Oauth
HLAA-05	Do you support differentiation between email address and user identifier?	Yes	One email can be associated with multiple accounts.
HLAA-06	Do you allow the customer to specify attribute mappings for any needed information beyond a user identifier? [e.g., Reference eduPerson, ePPA/ePPN/ePE]	Yes	Group information
HLAA-07	Are audit logs available to the institution that include AT LEAST all of the following; login, logout, actions performed, timestamp, and source IP address?	Yes	See the ArcGIS Online History API
HLAA-08	If you don't support SSO, does your application and/or user-frontend/portal support multi-factor authentication? (e.g. Duo, Google Authenticator, OTP, etc.)	Yes	SSO is supported, but MFA can be used with ArcGIS Online built-in accounts
HLAA-09	Does your application automatically lock the session or log-out an account after a period of inactivity?	No	ArcGIS Online is sessionless
Systems Management		**Vendor Answers**	**Additional Information**
HLSY-01	Do you have a systems management and configuration strategy that encompasses servers, appliances, cloud services, applications, and mobile devices (company and employee owned)?	Yes	Systems in the ArcGIS Online solution are managed in alignment with FedRAMP Tailored Low requirements, which include regular operating system updates and hot fixes. Any hardware updates are performed by the CSP.
HLSY-02	Will the institution be notified of major changes to your environment that could impact the institution's security posture?	Yes	See status page of trust.arcgis.com
HLSY-03	Are your systems and applications scanned for vulnerabilities [that are then remediated] prior to new releases?	Yes	Vulnerability assessments against ArcGIS Online are conducted at least monthly as part of the Continuous Monitoring Plan - including system, web application and database scans.

HLSY-04	Have your systems and applications had a third party security assessment completed in the last year?	Yes	A third party assessment was completed and a summary of the results can be made available upon request under NDA.
HLSY-05	Do you have policy and procedure, currently implemented, guiding how security risks are mitigated until patches can be applied?	Yes	In alignment with FedRAMP Moderate requirements.
Data		**Vendor Answers**	**Additional Information**
HLDA-01	Does the environment provide for dedicated single-tenant capabilities? If not, describe how your product or environment separates data from different customers (e.g., logically, physically, single tenancy, multi-tenancy)	No	ArcGIS Online utilizes logically separate production and non-production environments (environment is not physically separate). Separate SQL Azure databases to store hosted feature service data for each customer's ArcGIS Online
HLDA-02	Is sensitive data encrypted, using secure protocols/algorithms, in transport? (e.g. system-to-client)	Yes	ArcGIS Online provides encryption at REST with AES-256, and encryption in transit with HTTPS via TLS 1.2.
HLDA-03	Is sensitive data encrypted, using secure protocols/algorithms, in storage? (e.g. disk encryption, at-rest, files, and within a running database)	Yes	Data is encrypted at rest with AES-256 which is a FIPS 140-2 compliant encryption algorithms. This is in alignment with FedRAMP Tailored Low requirements
HLDA-04	Are involatile backup copies made according to pre-defined schedules and securely stored and protected?	Yes	Esri does backup infrastructure data and customer is responsible for backup of their data at whatever frequency they desire. Data is encrypted at rest with AES-256 which is a FIPS 140-2 compliant encryption algorithms. This is in alignment with FedRAMP Tailored Low requirements
HLDA-05	Can the Institution extract a full or partial backup of data?	Yes	Esri performs backup of infrastructure data and customer is responsible for backup of their data
HLDA-06	Do you have a media handling process, that is documented and currently implemented that meets established business needs and regulatory requirements, including end-of-life, repurposing, and data sanitization procedures?	Yes	AGO as a SaaS does not handle physical media. This is a responsibility of the Cloud infrastructure Provider (AWS and Azure)
HLDA-07	Does your staff (or third party) have access to Institutional data (e.g., financial, PHI or other sensitive information) within the application/system?	Yes	Select Esri system administraion staff have direct access to customer data and their actions fully logged. Customer remains responsible for their data and must have their own policies in place to avoid copying onto removable media. Third party cloud providers will have systems and procedures in place to prevent this copying, by restricting access to data centres and not permitting removable media within the data centres.
Datacenter		**Vendor Answers**	**Additional Information**
HLDC-01	Does your company manage the physical data center where the institution's data will reside?	No	ArcGIS Online utilized only AWS and MS Azure datacenters located within the US, EU or Asia Pacific regions.
HLDC-02	Are you generally able to accomodate storing each institution's data within their geographic region?	Yes	ArcGIS Online customers can choose to store data in the US, EU or Asia Pacific regions.
HLDC-03	Does the hosting provider have a SOC 2 Type 2 report available?	Yes	SOC2 reports may be obtained directly from AWS and MS Azure.
HLDC-04	Does your organization have physical security controls and policies in place?	Yes	See Cloud infrastructure provider documentation for physical security controls
HLDC-05	Do you have physical access control and video surveillance to prevent/detect unauthorized access to your data center?	Yes	Cloud infrastructure provider physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors. No subcontractor access beyond cloud providers
Networking		**Vendor Answers**	**Additional Information**
HLNT-01	Do you enforce network segmentation between trusted and untrusted networks (i.e., Internet, DMZ, Extranet, etc.)?	Yes	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.
HLNT-02	Are you utilizing a stateful packet inspection (SPI) firewall?	Yes	Cloud native firewall protections are utilized which provide stateful security groups.

HLNT-03	Do you use an automated IDS/IPS system to monitor for intrusions?	Yes	CSP's have their own IDS/IDP's in place. Anti-virus deployed to admin systems as well as any systems consuming external information sets.
HLNT-04	Are you employing any next-generation persistent threat (NGPT) monitoring?	Yes	ArcGIS Online utilizes native cloud service providers next gen threat assessment capabilities
HLNT-05	Do you require connectivity to the Institution's network for support/administration or access into any existing systems for integration purposes?	No	
Incident Handling		**Vendor Answers**	**Additional Information**
HLIH-01	Do you have a formal incident response plan?	Yes	Assessed by a 3rd party annually.
HLIH-02	Do you have an incident response process and reporting in place to investigate any potential incidents and report actual incidents?	Yes	Incident management is delineated within ArcGIS Online's Incident Response Plan documentation aligning with FedRAMP Tailored Low requirements.
HLIH-03	Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?	Yes	Esri has cyber liability insurance and general liability insurance details can be shared under NDA.
HLIH-04	Do you have either an internal incident response team or retain an external team?	Yes	Internal incident response team is in place for both products and corporate operations
HLIH-05	Do you have the capability to respond to incidents on a 24x7x365 basis?	Yes	Cloud providers have 24x7 SOCs and Esri monitors for application relatied issues.
Policies, Procedures, and Processes		**Vendor Answers**	**Additional Information**
HLPP-01	Can you share the organization chart, mission statement, and policies for your information security unit?	Yes	Please review our Trust Center here: https://trust.arcgis.com/en/ Policy TOC may be shared under NDA. See our ArcGIS Security Development Lifecycle documentation: https://downloads.esri.com/RESOURCES/ENTERPRISEGIS/Esri_SDLC.pdf
HLPP-02	Are information security principles designed into the product lifecycle?	Yes	See our ArcGIS Security Development Lifecycle documentation: https://downloads.esri.com/RESOURCES/ENTERPRISEGIS/Esri_SDLC.pdf
HLPP-03	Do you have a documented information security policy?	Yes	Our policy Table of Contents may be shared under NDA.
Third Party Assessment			**Additional Information**
HLTP-01	Will institution data be shared with or hosted by any third parties? (e.g. any entity not wholly-owned by your company is considered a third-party)	Yes	ArcGIS Online infrastructure is hosted in AWS and MS Azure datacenters located within the United States
HLTP-02	Do you perform security assessments of third party companies with which you share data? (i.e. hosting providers, cloud services, PaaS, IaaS, SaaS, etc.).	Yes	A third party assessments performed anually as part of FedRAMP requirements.
HLTP-03	Do you have an implemented third party management strategy?	Yes	Management strategy of 3rd parties audited for alignment with FedRAMP requirements annually.
HLTP-04	Do you have a process and implemented procedures for managing your hardware supply chain? (e.g., telecommunications equipment, export licensing, computing devices)	Yes	Esri does, but for AGO, since it is a SaaS, we do not handle hardware. This is managed by the Cloud infrastructure Provider