Compliance with security and privacy standards and regulations

When it comes to cloud service providers, it is in A.SPIRE's best interest to perform due diligence on vendor's compliance with applicable industry standards and regulations for the hosting of the SPIRE Knowledge Platform. This page summarizes current cloud service provider's compliance with the following standards and regulations:

SOC 1 (SSAE No. 16 and ISAE No. 3402)

Statement on Standards for Attestation Engagement (SSAE) No. 16 is an American auditing standard issued by the American Institute of Certified Public Accountants (AIPCA) and is used to create a Service Organization Control (SOC) 1 branded report. Our cloud service provider's SSAE 16 audit report is aligned with the International Standards for Assurance Engagements (ISAE) No. 3402 auditing standard. This allows for the report to be recognized both in the U.S. and throughout the world.

Our cloud service provider has a SOC 1 SSAE 16/ISAE 3402 Type 2 audit performed on an annual basis by an independent third-party audit firm. The audit report attests to the design and operating effectiveness of business and security controls in safeguarding systems and data. Our cloud service provider's SSAE 16/ISAE 3402 audit report is available to current customers and prospective customers upon request and with a fully executed non disclosure agreement (NDA).

SOC 2

A SOC 2 report, titled "Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy" is designed to meet a broad set of reporting needs about the controls at a service organization in the form of a CPA firm's independent attestation report. SOC 2 reports are based on the following AICPA Trust Services Principles and Criteria (TSPC):

- *Security* - The system is protected against unauthorized access (both physical and logical).
- *Availability* - The system is available for operation and use as committed or agreed.
- *Processing Integrity* - System processing is complete, accurate, timely, and authorized.
- *Confidentiality* - Information designated as confidential is protected as committed or agreed.

- *Privacy* - Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in Generally Accepted Privacy Principles issued by the AICPA and CICA. The TSPC of security, availability, and processing integrity are used to evaluate whether a system is reliable.

It also has a SOC 2 Type 2 audit performed on an annual basis by an independent third party audit firm. The audit report attests to the suitability of the design and operating effectiveness of controls to meet the Security, Availability and Confidentiality Trust Services Principles. Our cloud service provider's SOC 2 audit report is available to current customers and prospective customers upon request and with a fully executed NDA.

PCI

Payment Card Industry Data Security Standard (PCI DSS) compliance applies to merchants and services providers that process, store, or transmit credit card data. PCI DSS is a multifaceted security standard that includes requirements for security management, policies and procedures, network architecture, software design, and other critical protective measures. This comprehensive standard helps organizations proactively protect credit card data that is transmitted or stored on the platform. PCI compliance is only applicable to customers that build web applications within the shared PCI Virtual Private Cloud (VPC) or via dedicated PCI VPC Shield offering.

Our cloud service provider has been validated by an independent Quality Security Assessor (QSA) approved by the PCI Security Standards Council that validated adherence with standards applicable to a Level 1 service provider under PCI DSS Version 3.1.

For information about Amazon's PCI accreditation, see http://aws.amazon.com/compliance/pci-dss-level-1-faqs/ .

ISO 27001 certification

Our cloud service provider is ISO 27001 certified. You can download our certificate here . ISO 27001 is a globally recognized security standard driven by the implementation of an information security management system (ISMS). An ISMS is a security framework of policies, procedures and controls that includes administrative, physical and technical safeguards to manage information security risks to internal and customer information.

FedRAMP

Our cloud service provider must be a Federal Risk Authorization and Management Program (FedRAMP) compliant system and has received an agency Authority to Operate (ATO) from the Department of the Treasury. As a FedRAMP compliant Cloud Service Provider (CSP) supporting U.S. government agencies and departments, the provider is committed to meeting the guidelines of FedRAMP and will provide insight into the provider's security architecture and the continuous monitoring processes related to the Platform as a Service (PaaS).

Our system has been designed to meet NIST 800-53 standards for customers who must complete their local security authorization process, sometimes called the Risk Management Framework (RMF), or FISMA.

In addition, our Cloud is built on Amazon AWS and thus inherits Infrastructure layer controls from Amazon. Separately, Amazon AWS has received FedRAMP authorization for the Infrastructure layer.

FISMA

The provider enables US government agencies to achieve and sustain compliance with FISMA. Numerous Federal organizations have successfully achieved security authorizations and made risk-based decisions to allow websites to be hosted on the provider's Cloud in accordance with the Risk Management Framework (RMF) process defined in the NIST Special Publication (SP) 800-37. Our cloud service provider's platform has helped federal agencies expand cloud computing use cases and deploy sensitive government data and applications in the cloud, while complying with the rigorous security requirements of federal standards.

CSA STAR

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The CSA is led by a broad coalition of industry practitioners, corporations, associations, and other key stakeholders.

CSA's Security, Trust and Assurance Registry (STAR) is a free, publicly accessible registry that documents the security controls provided by cloud computing offerings, thereby helping organizations assess the security of cloud providers they currently use or are considering contracting with. The provider has completed and published its Consensus Assessments Initiative Questionnaire (CAIQ), which provides industry-accepted ways to document the security controls in our PaaS (platform as a service) offering. The CAIQ provides a set of over 140 questions that a cloud consumer and cloud auditor may wish to ask of a cloud provider.

CAIQ is available for download from the CSA STAR registry.

Safe Harbor

Safe Harbor is a certification program run by the US Department of Commerce that aims to harmonize data privacy practices between the US and the stricter privacy regulations of the European Union (EU). The provider was registered with the Safe Harbor program on February 7, 2012.

To view certification with Safe Harbor, see http://safeharbor.export.gov/companyinfo.aspx?id=22159.

EU cookie regulations

The Privacy and Electronic Communications Regulations 2003 (a European Community (EC) Directive) cover the use of cookies and similar technologies for storing information and accessing information stored on users' equipment, such as their computer or mobile phone. In 2009, this Directive was amended by Directive 2009/136/EC. This included a change to Article 5(3) of the E-Privacy Directive requiring consent before a website stores cookies or similar technologies.

Privacy

The provider abides by all privacy laws and regulations that are applicable to our hosting services and to our customers that host websites that may contain personal information on this Cloud. The provider personnel have logical access to customer data stored in customer websites only if they are authorized, and have a need for access due to their job function. The provider does not transfer customer data hosted on the Cloud outside of the Cloud or to any third party without customer authorization.

Customers must ensure that privacy concerns and regulations are addressed and adhered to at the application layer where customer personnel may have logical access to personal information uploaded or stored in customer websites.

The provider's Privacy Policy describes how it handles any personal information gathered from visitors to its website and from users of our software and services.