**APPLICATION**

1. Describe the underlying technology of the application or service (including programming language, operating system and database software).
   1. The application is primarily written in Python (Django framework) (<https://en.wikipedia.org/wiki/Bitbucket> see “Written in”)
   2. List of hardware requirements mentioning all compatible databases and tools can be seen here: <https://confluence.atlassian.com/bitbucketserver/supported-platforms-776640981.html>
2. Describe the mechanism that will be used to transmit information between end user and backend system. Please include authentication, authorization, transport layer and session tracking information.
3. What security control(s) are in place to prevent unauthorized access to the application?
   1. HTTPS is required,
   2. Improved SSH (<https://blog.bitbucket.org/2016/08/10/ssh-improvements-bitbucket-cloud/> )
   3. Two-step verification (<https://blog.bitbucket.org/2015/09/10/two-step-verification-is-here/?utm_source=BB-blog&utm_medium=social&utm_campaign=bitbucket_fy17q1-momentum-posts> )
   4. U2F (<https://blog.bitbucket.org/2016/06/22/universal-2nd-factor/> )

**INFRASTRUCTURE**

1. Describe at a high level the infrastructure that the application and system are hosted on, including server (physical and virtual), network and storage? Please provide network diagram.
   1. Atlassian utilizes NTT colocation services for all commercial hosting needs. They are a premier provider of fully-managed hosting service. (<https://www.atlassian.com/licensing/cloud/evaluation#overview-2> see “Is my data secure?” )
      1. Infrastructure (see <https://www.nttict.com/services/infrastructure/> )
      2. Security whitepaper and SLA (see <https://www.us.ntt.net/support/sla/network.cfm> )
   2. It is a cloud based infrastructure with data centers in geographically diverse locations across the United States (<https://www.atlassian.com/trust/policies/cloud-security> see Facilities)
   3. Status of the services: <https://status.bitbucket.org/?_ga=1.68457624.825906834.1477511281>
2. How many datacenters do you have and where are they located? (if applicable)
   1. Our data centres are located in geographically diverse locations across the United States (<https://www.atlassian.com/trust/policies/cloud-security> see Facitlities)
3. Does your organization undergo any annual 3rd party assurance review or audit such as SSAE 16 SOC 2, PCI?
   1. Our data centers are SOC-1 (formerly SAS 70) compliant. These certifications address physical security, system availability, network and IP backbone access, customer provisioning and problem management.

Our Cloud operations and security have been evaluated against the Cloud Security Alliance (CSA) standard and our self-assessment can be found on the Atlassian CSA STAR Registry entry.

(<https://www.atlassian.com/trust/policies/cloud-security> see Ceertification)

**DATA**

1. Describe the information that will be captured. Provide example.
   1. (<https://www.atlassian.com/legal/privacy-policy> see “Information you provide to us”, “Information we collect from your use of Atlassian Services”, “Information we collect from other sources”)
2. How will the information be transmitted? E.g. TLS, SFTP, etc.
   1. HTTPS (<https://www.atlassian.com/legal/privacy-policy> see “Data storage, transfer and security”)
3. How will the information be stored and secured? E.g. disk encryption, database encryption
   1. Application database backups for Atlassian Cloud occur on the following frequencies: On-site backups are performed daily and retained for seven days; Tape backups are taken weekly, which are then stored off-site and retained for four weeks. All backup data is encrypted. (<https://www.atlassian.com/trust/policies/cloud-security> see “Backups”)
   2. (<https://www.atlassian.com/legal/privacy-policy> see “Data storage, transfer and security”)

**SECURITY ASSESSMENT**

1. Do you undergo regular **penetration or vulnerability testing** of your infrastructure and application? If yes, were they performed by a third party?
   1. CSA (Cloud Security Alliance) self-assessment: <https://downloads.cloudsecurityalliance.org/star/self-assessment/atlassian-caiq-v3.0.1-2016-09-30.xlsx.zip>
   2. Third party penetration testing: yes. (<https://www.atlassian.com/trust/policies/cloud-security> see “Certification”)
2. What security control(s) are in place to **detect and/or prevent** unauthorized access to your infrastructure environment? (i.e. firewalls, IDS/IPS, antivirus, SIEM, WAF)
   1. (<https://www.atlassian.com/trust/policies/cloud-security> see “People and access”)
3. Do you have security policies and/or procedures on Security Incident Response Plan, Disaster Recovery Plan, Change Management, and Patch Management)? If yes, would you be able to provide a copy?
   1. CSA (Cloud Security Alliance) self-assessment: <https://downloads.cloudsecurityalliance.org/star/self-assessment/atlassian-caiq-v3.0.1-2016-09-30.xlsx.zip>