Report on Atlassian Corporation Plc's Description of Its Confluence Databases and Confluence Whiteboards Features and on the Suitability of the Design of Its Controls Relevant to Security, Availability, and Confidentiality and HIPAA Security and Breach Notification Rules as of February 29, 2024

SOC 2® - SOC for Service Organizations: Trust Services Criteria + HIPAA Security and Breach Notification Rules

Confluence Databases | Confluence Whiteboards

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Atlassian Corporation Plc ("Atlassian")

Scope

We have examined Atlassian's accompanying description of its Confluence Databases and Confluence Whiteboards Features found in Section 3 titled "Atlassian Corporation Plc's Description of Its Confluence Databases and Confluence Whiteboards Features as of February 29, 2024" (description), based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022*) (2018 description criteria), and the suitability of the design of controls stated in the description as of February 29, 2024, to provide reasonable assurance that Atlassian's service commitments and system requirements would be achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (2017 TSC). We have also examined whether controls were implemented to meet the requirements set forth in Sections § 164.308, § 164.310, § 164.312, § 164.314, § 164.316, § 164.410, § 164.412, and § 164.414 of the Healthcare Insurance Portability and Accountability Act Security and Breach Notification Rules (HIPAA criteria).

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Atlassian, to achieve Atlassian's service commitments and system requirements based on the applicable trust services and HIPAA criteria. The description presents Atlassian's controls, the applicable trust services and HIPAA criteria, and the complementary user entity controls assumed in the design of Atlassian's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Atlassian uses subservice organizations to provide data center colocation services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Atlassian, to achieve Atlassian's service commitments and system requirements based on the applicable trust services and HIPAA criteria. The description presents Atlassian's controls, the applicable trust services and HIPAA criteria, and the types of complementary subservice organization controls assumed in the design of Atlassian's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Atlassian is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Atlassian's service commitments and system requirements would be achieved. In Section 2, Atlassian has provided the accompanying assertion titled "Assertion of Atlassian Corporation Plc Management" (assertion) about the description and the suitability of the design of controls stated therein. Atlassian is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the

risks that threaten the achievement of the service organization's service commitments and system requirements. Atlassian is also responsible for selecting the applicable HIPAA criteria as additional criteria and implementing controls to meet the Security and Breach Notification Rules set forth in the HIPAA criteria.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria.

We are also responsible for expressing an opinion about whether the controls stated in the description were implemented to meet the Security and Breach Notification Rules set forth in the HIPAA criteria based on our examination. Attestation standards established by the American Institute of Certified Public Accountants require that we also plan and perform our examination to obtain reasonable assurance about whether, in all material respects, Atlassian implemented controls to meet the Security and Breach Notification Rules set forth in the HIPAA criteria.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

An examination of a description of a service organization's system and the suitability of the design of controls, and the implementation of controls to meet the Security and Breach Notification Rules set forth in the HIPAA criteria involves—

- Obtaining an understanding of the system and the service organization's service commitments and system requirements and HIPAA criteria.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether the controls stated in the description were implemented to meet the Security and Breach Notification Rules set forth in the HIPAA criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects—

a. The description presents Atlassian's Confluence Databases and Confluence Whiteboards Features that were designed and implemented as of February 29, 2024, in accordance with the description criteria.

b. The controls stated in the description were suitably designed as of February 29, 2024, to provide reasonable assurance that Atlassian's service commitments and system requirements would be achieved based on the applicable trust services and HIPAA criteria, if its controls operated effectively as of that date and if the subservice organizations and user entities applied the complementary controls assumed in the design of Atlassian's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Atlassian , user entities of Atlassian's Confluence Databases and Confluence Whiteboards Features as of February 29, 2024, business partners of Atlassian subject to risks arising from interactions with Atlassian's Confluence Databases and Confluence Whiteboards Features, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The Security and Breach Notification Rules of the HIPAA criteria.

- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties. If a report recipient is not a specified party as defined above and has obtained this report, or has access to it, use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Coalfire Controls, LLC as a result of such access. Further, Coalfire Controls, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Coalfire Controls LLC

Greenwood Village, Colorado
April 26, 2024

Section 2

Assertion of Atlassian Corporation Plc Management

Assertion of Atlassian Corporation Plc ("Atlassian") Management

We have prepared the accompanying description of the Confluence Databases and Confluence Whiteboards Features titled "Atlassian Corporation Plc's Description of Its Confluence Databases and Confluence Whiteboards Features as of February 29, 2024" (description), based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* (2018 description criteria). The description is intended to provide report users with information about the Confluence Databases and Confluence Whiteboards Features that may be useful when assessing the risks arising from interactions with Atlassian's system, particularly information about system controls that Atlassian has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (2017 TSC) and the requirements set forth in Sections § 164.308, § 164.310, § 164.312, § 164.314, § 164.316, § 164.410, § 164.412, and § 164.414 of the Healthcare Insurance Portability and Accountability Act Security and Breach Notification Rules (HIPAA criteria), as stated in the description.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Atlassian, to achieve Atlassian's service commitments and system requirements based on the applicable trust services and HIPAA criteria. The description presents Atlassian's controls, the applicable trust services and HIPAA criteria, and the complementary user entity controls assumed in the design of Atlassian's controls.

Atlassian uses subservice organizations for data center colocation services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Atlassian, to achieve Atlassian's service commitments and system requirements based on the applicable trust services and HIPAA criteria. The description presents Atlassian's controls, the applicable trust services and HIPAA criteria, and the types of complementary subservice organization controls assumed in the design of Atlassian's controls. The description does not disclose the actual controls at the subservice organizations.

We confirm, to the best of our knowledge and belief, that:

a. The description presents Atlassian's Confluence Databases and Confluence Whiteboards Features that were designed and implemented as of February 29, 2024, in accordance with the description criteria.

b. The controls stated in the description were suitably designed as of February 29, 2024, to provide reasonable assurance that Atlassian's service commitments and system requirements would be achieved based on the applicable trust services and HIPAA criteria, if its controls operated effectively as of that date, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Atlassian's controls as of that date.

Vikram Rao
Chief Trust Officer
Atlassian Corporation Plc

Section 3

Atlassian Corporation Plc's Description of Its Confluence Databases and Confluence Whiteboards Features as of February 29, 2024

Type of Services Provided

Company Overview and Background

Atlassian Corporation Plc (“Atlassian” or “the Company”) was established in 2002 and had its initial public offering (IPO) in 2015. Atlassian has employees working remotely across various countries, with offices around the world including the United States (San Francisco, Mountain View, New York City, Austin, Boston), Australia (Sydney), Philippines (Manila), Japan (Yokohama), Netherlands (Amsterdam), Poland (Gdansk), Turkey (Ankara), and India (Bengaluru).

Atlassian's collaboration software helps teams organize, discuss, and complete shared work. Teams across large and small organizations worldwide use Atlassian's project tracking, content creation and sharing, real-time communication, and service management products to work together. Atlassian provides a range of products and features including Confluence Databases and Confluence Whiteboards.

This report focuses on the key operating systems that constitute the products and features hosted on Amazon Web Services (AWS) for all in-scope systems along with the supporting information technology (IT) infrastructure and business processes. It does not include on-premise versions, service enhancements that are not explicitly defined, add-ons obtained from the marketplace, or open-source downloadable software added by customers to their instance.

Overview of In-Scope Products and Features

The system description in this section of the report details Confluence Databases and Confluence Whiteboards (“the Systems”). Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organizations).

The scope of this report includes features (components of the system that provide enhanced functionality) that operate as part of an existing Atlassian Cloud product.

Confluence Databases

Confluence Databases is a feature that enables users to collaborate on databases within Confluence.

Confluence Whiteboards

Confluence Whiteboards is a feature for Confluence that enables users to collaborate on an infinite virtual whiteboard.

Principal Service Commitments and System Requirements

Atlassian designs its processes and procedures to align with the objectives of Confluence Databases and Confluence Whiteboards. These objectives are formulated according to the service commitments made by Atlassian to user entities; the laws and regulations governing the provision of the Systems; and the financial, operational, and compliance requirements that Atlassian has established for the Systems.

The commitments to user entities regarding security, availability, and confidentiality are documented and communicated through various channels, such as the Atlassian Customer Agreement, Product-Specific Terms of Services, the sign-up page, Privacy Policy, and Atlassian Trust Center. The commitments to security, availability, and confidentiality include, but not limited to:

Trust Services Category	Service Commitments
Security	• Atlassian will implement and maintain physical, technical, and administrative security measures designed to protect customer data from unauthorized access, destruction, use, modification, or disclosure. • Atlassian will maintain a compliance program that includes independent third-party audits and certifications. • Atlassian will notify customers without undue delay upon becoming aware of a security incident.
Availability	• Atlassian will use commercially reasonable efforts to maintain the availability of the products.
Confidentiality	• Atlassian will not disclose confidential information to any third party unless they have a business need to know. • Atlassian will not use confidential information for any purpose other than providing the services. • Atlassian will delete or return customer data in accordance with the retention periods upon termination of the services.

Atlassian establishes operational requirements that support the achievement of its security, availability, and confidentiality commitments as well as relevant laws and regulations and other system requirements. These requirements are communicated through Atlassian's system policies and procedures, system design documentation, and contracts with customers. Atlassian's information security policies define an organization-wide approach to protecting systems and data. These policies include those related to the design and development of services, operation of the systems, management of internal business systems and networks, and employee hiring and training. Standard operating procedures have been documented for carrying out specific manual and automated processes required for the operation and development of Confluence Databases and Confluence Whiteboards.

Components of the System Used

The boundaries of Confluence Databases and Confluence Whiteboards refer to the aspects of the Company's infrastructure, software, personnel, procedures, and data that are essential for providing its services and that directly contribute to the services offered to customers. The sections below provide a description of the components that directly support the services offered to customers. Any infrastructure, software, personnel, procedures, or data that provide support indirectly are not included.

Infrastructure

Confluence Databases and Confluence Whiteboards utilize AWS data centers and infrastructure-as-a-service (IaaS). Atlassian administrators oversee virtual server and operating system configurations through distinct AWS accounts and configuration management processes.

Features are deployed in various regions to ensure redundancy and fault tolerance, including:

Infrastructure – Features			
Feature	AWS Region		
	United States (US)	Europe (EU)	Asia Pacific (AP)
Confluence Databases	✓	✓	✓
Confluence Whiteboards	✓	✓	✓

Network

Atlassian has public ingress points in multiple AWS regions. These traffic manager clusters terminate public Transport Layer Security (TLS) and forward the requests to proxies hosted in AWS regions. All AWS-hosted network traffic is inside the Atlassian Cloud Network and all traffic in and between AWS regions uses AWS Transit Gateway or Amazon Virtual Private Cloud (Amazon VPC) peering. Encryption in transit is implemented to protect user authentication information and the corresponding session transmitted over the Internet or other public networks to ensure that data reaches its intended destination.

Cloudflare is an additional public data ingress point (alongside AWS) that is used for the ingestion and distribution of real-time messages for users collaborating on Confluence Whiteboards and Confluence Databases. Cloudflare sits behind its own third-party firewall, which has been configured with the same rules configured in Atlassian's Global Edge firewall that protects the corporate network.

Connections to features and products are protected using secure connectivity protocols. At all points, the network traffic is encrypted with TLS version 1.2 or higher. Traffic between Atlassian’s environment and Cloudflare uses the same Global Edge firewall configuration that protects the corporate network.

Advanced Encryption Standard (AES)-256 is enabled to ensure encryption at rest within all data stores of Atlassian products and key services.

Upon accepting the terms and conditions and completing the sign-up flow, a new database record and unique identifier are created for a customer account. The unique ID is used thereafter for associating data with the specific customer account. Configurations are in place to ensure that the ID is automatically assigned and unique. The data is logically separated from other customer data using the unique IDs. No database details are used for multiple cloud IDs to ensure this segregation between customers.

A Zero Trust infrastructure is implemented to place endpoints into a tiered network (High, Low, Open) based on their security posture and the type of device. Applications added to the single sign-on (SSO) platform are tiered according to the Zero Trust policy. Endpoints cannot access applications via the SSO platform unless they are placed on the same (or higher) tier as the application. High-tier applications have security requirements that include, but are not limited to, effective malware protection, local drive encryption, and up-to-date operating system versions.

Firewall rules have been implemented and policy rules have been configured to restrict access to unnecessary ports, protocols, and services. Atlassian has implemented company-wide firewall rules that are managed centrally by the Platform and Enterprise Cloud Team. Individual products and features manage key Internet Protocol (IP) ports security policy roles to ensure that only authorized ports are in use. Any changes to firewall rules at the Global Edge, product, or service level must go through a peer review and approval process.

Database

Atlassian products utilize logically separate databases for each product instance. The data is segregated by tenant at the application layer using a unique identifier to query customer data.

The databases implemented by Atlassian include independent synchronous replicas in multiple availability zones (AZs) within the same region to mitigate the risk of data loss due to hardware failure. The primary datastore used within the Atlassian environment consists of Amazon Relational Database Service (Amazon RDS) clusters located within the private network hosted in AWS. The cluster is shared, and its nodes are distributed across multiple AZs to provide fault tolerance and redundancy.

Backups are retained at a minimum for 30 days to provide redundancy and enable point-in-time data recovery (PITR). The data is stored in both the document storage platform (Media Platform) and Amazon Simple Storage Service (Amazon S3). Amazon S3 is utilized as a file service for user attachments, backups, and log archives and is the operational responsibility of Amazon.

Confluence Whiteboards and Confluence Databases further use Cloudflare Workers KV for temporary metadata storage and Cloudflare Workers Durable Objects for temporary storage of user-generated content while data is in-transit.

Software

The following table lists the software, services, and tools that support the control environment of Confluence Databases and Confluence Whiteboards:

Function	Name	Component
Hosting Systems	Amazon Elastic Compute Cloud (Amazon EC2)	Confluence Databases, Confluence Whiteboards
	Kubernetes on top of Amazon EC2	Confluence Databases, Confluence Whiteboards
	CentOS	Confluence Databases, Confluence Whiteboards
	Lambda	Confluence Databases, Confluence Whiteboards
	Lambda@Edge	Confluence Databases, Confluence Whiteboards
Storage and Database	Dynamo Database	Confluence Databases, Confluence Whiteboards
	Amazon S3	Confluence Databases, Confluence Whiteboards
	Amazon S3 Glacier	Confluence Databases, Confluence Whiteboards
	Cloudflare Workers KV	Confluence Databases, Confluence Whiteboards
	Cloudflare Workers Durable Objects	Confluence Databases, Confluence Whiteboards
Network	Amazon VPC	Confluence Databases, Confluence Whiteboards
	Amazon Application Load Balancers (ALBs)	Confluence Databases, Confluence Whiteboards
	Cloudflare	Confluence Databases, Confluence Whiteboards
	Corporate firewall	Confluence Databases, Confluence Whiteboards
	Amazon CloudFront	Confluence Databases, Confluence Whiteboards

Function	Name	Component
	AWS Web Application Firewall (AWS WAF)	Confluence Databases, Confluence Whiteboards
Messaging	Amazon Simple Queue Service (Amazon SQS)	Confluence Databases, Confluence Whiteboards
	Cloudflare Workers Durable Objects	Confluence Databases, Confluence Whiteboards
	Slack	Confluence Databases, Confluence Whiteboards
Build, Release, and Continuous Integration Systems	Bitbucket Cloud	Confluence Databases, Confluence Whiteboards
	Bitbucket Pipelines	Confluence Databases, Confluence Whiteboards
	Tokenator	Confluence Databases, Confluence Whiteboards
Access Management	Active Directory (AD)	Confluence Databases, Confluence Whiteboards
	CyberArk Idaptive SSO	Confluence Databases, Confluence Whiteboards
	CyberArk Workforce Password Management	Confluence Databases, Confluence Whiteboards
	Duo two-factor authentication (2FA)	Confluence Databases, Confluence Whiteboards
	1Password	Confluence Databases, Confluence Whiteboards
Monitoring and Alerting	AWS CloudTrail	Confluence Databases, Confluence Whiteboards
	Cloudflare Log Push	Confluence Databases, Confluence Whiteboards
	Opsgenie	Confluence Databases, Confluence Whiteboards
	Pollinator	Confluence Databases, Confluence Whiteboards
	SignalFX	Confluence Databases, Confluence Whiteboards
	Splunk	Confluence Databases, Confluence Whiteboards
	Sentry	Confluence Databases, Confluence Whiteboards
Customer Support and Communication	Intercom	Confluence Databases, Confluence Whiteboards
	Statuspage	Confluence Databases, Confluence Whiteboards
Vulnerability Scanning	Cloud Conformity	Confluence Databases, Confluence Whiteboards
	BugCrowd	Confluence Databases, Confluence Whiteboards
	CrowdStrike	Confluence Databases, Confluence Whiteboards
	Tenable	Confluence Databases, Confluence Whiteboards
	Snyk	Confluence Databases, Confluence Whiteboards
	Security Assistant	Confluence Databases, Confluence Whiteboards

Function	Name	Component
Human Resources (HR)	Workday	Confluence Databases, Confluence Whiteboards
	Lever	Confluence Databases, Confluence Whiteboards
Learning, Training, and Development	Absorb	Confluence Databases, Confluence Whiteboards
	Learning Central	Confluence Databases, Confluence Whiteboards
	Haekka	Confluence Databases, Confluence Whiteboards
	Degreed	Confluence Databases, Confluence Whiteboards
	Get Abstract	Confluence Databases, Confluence Whiteboards
	LinkedIn Learning	Confluence Databases, Confluence Whiteboards
	Learndot	Confluence Databases, Confluence Whiteboards
	Intellum	Confluence Databases, Confluence Whiteboards
Notifications	Nexmo	Confluence Databases, Confluence Whiteboards
	Mailgun	Confluence Databases, Confluence Whiteboards
	Twilio	Confluence Databases, Confluence Whiteboards
	Pubnub	Confluence Databases, Confluence Whiteboards
	SES	Confluence Databases, Confluence Whiteboards
Asset Management	Jamf Pro	Confluence Databases, Confluence Whiteboards
	Workspace One	Confluence Databases, Confluence Whiteboards
	Bitlocker	Confluence Databases, Confluence Whiteboards
	Filevault	Confluence Databases, Confluence Whiteboards

AWS and Cloudflare are third-party vendors that provide physical and environmental safeguards, infrastructure support, management, and storage services. Atlassian has identified the complementary subservice organization controls of AWS and Cloudflare to achieve the applicable trust services criteria.

The other third-party vendors mentioned above are only applicable to support specific controls.

People

The Company develops, manages, and secures Confluence Databases and Confluence Whiteboards via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Co-Founders and Executive Management	Responsible for overseeing company-wide initiatives, establishing and accomplishing goals, and managing objectives

People	
Group/Role Name	**Function**
People (in partnership with the people leaders)	Responsible for determining career growth and performance strategy, talent acquisition, continuing education paths, total rewards, and workplace experiences
Finance	Responsible for financial, accounting, tax, internal audit, investor relations, procurement, and treasury
Legal	Responsible for matters related to corporate development, confidentiality, general counsel operations, and public relations
Trust	Responsible for managing access controls, the security of the production environment, enterprise risk management, business continuity, and compliance for Confluence Databases and Confluence Whiteboards
Engineering	Responsible for the development, testing, deployment, and maintenance of new code for Confluence Databases and Confluence Whiteboards
Platform and Enterprise Cloud	Responsible for architecting, building, and maintaining Confluence Databases and Confluence Whiteboards
Ecosystem	Responsible for third-party connectivity platforms and applications
Foundation	Responsible for promoting diversity, equality, and inclusion in all organizations
Product	Responsible for overseeing the product life cycle, including adding new product functionality

The following organizational chart reflects the Company's internal structure related to the groups discussed above:

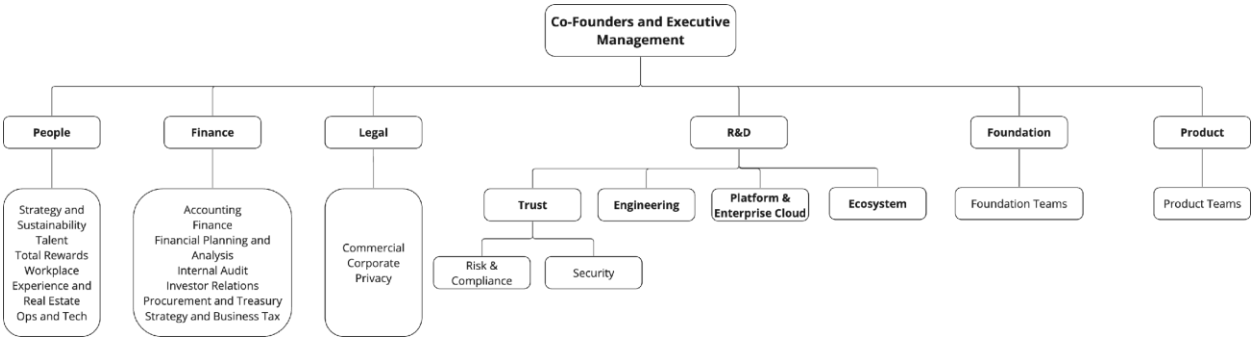

Figure 1: Atlassian Organizational Chart

Policies and Procedures

Atlassian maintains a Policy Management Program to help ensure that policies and procedures are:

- Properly communicated throughout the organization
- Properly owned, managed, and supported
- Clearly outlining business objectives
- Showing commitment to meet regulatory obligations

- Focused on continual iteration and improvement
- Providing for an exception process
- Supported by the Policy Framework and Structure

Atlassian defines policies, standards, guidelines, and procedures, and each document maintained by Atlassian is classified into one of these four categories based on the content of the document.

Policies, Standards, Guidelines, and Procedures		
Item	**Defines**	**Explanation**
Policy	General rules and requirements ("state")	Outlines specific requirements or rules that must be met.
Standard	Specific details ("what")	Collection of system-specific or procedural-specific requirements that must be met by all personnel.
Guideline	Common practice recommendations and suggestions	Collection of system-specific or procedural-specific "suggestions" for best practices. They are not requirements to be met but are strongly recommended. Effective policies make frequent references to standards and guidelines that exist within an organization.
Standard operating procedures	Steps to achieve Standard/Guideline requirements, in accordance with the rules ("actions")	A set of instructions on how to accomplish a task. From a compliance perspective, a procedure is also referred to as a Control Activity: the goal of a process/procedure is to help achieve a consistent outcome defined by the Standard or Guideline.

Policy Requirements

Every policy has a policy owner who is responsible for managing the risk outlined in the policy objective. All policies are reviewed, at least annually, to help ensure that they are relevant and appropriately manage risk in accordance with Atlassian's risk appetite. Changes are reviewed by the Atlassian Policy Committee (APC) and approved by the corresponding policy owner.

The APC reviews policy exceptions and violations and recommends actions to the policy owners and Executive Management team. Policy owners can approve exceptions for a period no longer than 1 year.

Policy Review Process

All policies, standards, guidelines, and standard operating procedures go through a review process to become available internally to all Atlassian employees. The review process follows Atlassian's internal process in which feedback is sought from a small group of knowledgeable peers on the topic. After feedback is incorporated, the draft document is submitted to the APC, either via email or via the internal corporate chat system. Any updates to policies, standards, or guidelines are shared via email and the internal website where all policies are stored.

Data Classification and Confidentiality of Information

All Atlassian employees share in the responsibility to safeguard information with an appropriate level of protection by observing the Data Classification policy:

- Information should be classified in terms of legal requirements, value, and criticality to Atlassian
- Information should be labeled to manage appropriate handling
- All removable media should be managed with the same handling guidelines as below
  - Media being disposed of should be securely deleted
  - Media containing company information should be protected against unauthorized access, misuse, or corruption during transport

Data Classification		
Rating	**Description**	**Examples**
Restricted	Information that would be very damaging, cause loss of trust with customers, and present legal risk to Atlassian and/or customers if mishandled	• Customer data • Sensitive company accounting data (e.g., non-public financial data, including consolidated revenue, expenses, cash flow, and earnings guidance prior to release) • Decryption keys, passwords, or other access control mechanisms protecting data at this level • United States Social Security Numbers (customers or employees) • Customer and employee Personally Identifiable Information (PII) • Employee personal, bank, and salary details
Protected	Information that could cause loss of trust with customers or present legal risk to Atlassian if mishandled	• Atlassian Account ID
Confidential	Information that would likely be damaging and could cause loss of trust with customers if mishandled	• Confidential personal data elements • Information related to business plans or deals • Information under a Non-Disclosure Agreement (NDA) • Descriptions of unresolved security issues in Atlassian products • Third-party closed-source code
Internal	Information internal to Atlassian that could be potentially damaging to Atlassian and/or customers if mishandled	• Most Confluence pages • Most information stored in Jira • Unreleased source code for Atlassian products • Unapproved drafts of public communications
Public	Data that is freely available to the public and presents no risk	• Approved public communications • Information on www.atlassian.com or other public web properties

System Incidents

There were no identified significant system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements as of February 29, 2024.

The Applicable Trust Services Criteria, Control Specifications Included in the Health Insurance Portability and Accountability Act (HIPAA) Security Rule and Breach Notification Rules, and Related Controls

Applicable Trust Services Criteria

The Trust Services Categories that are in scope for the purposes of this report are as follows:

- *Security*: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability or confidentiality of information or systems and affect the entity's ability to meet its objectives.
- *Availability*: Information and systems are available for operation and use to meet the entity's objectives.
- *Confidentiality*: Information designated as confidential is protected to meet the entity's objectives.

Many of the criteria used to evaluate a system are shared amongst all in-scope categories; for example, the criteria related to risk assessment apply to the security, availability, and confidentiality categories. As a result, the criteria for the security, availability, and confidentiality categories are organized into (a) the criteria that are applicable to all categories (common criteria) and (b) criteria applicable only to a single category. The common criteria constitute the complete set of criteria for the security category. For the categories of availability and confidentiality, a complete set of criteria is comprised of all the common criteria and all the criteria applicable to the category being reported on.

The common criteria are organized as follows:

1. *Control environment:* The criteria relevant to how the entity is structured and the processes the entity has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, qualifications of personnel, and the environment in which they function.
2. *Information and communication:* The criteria relevant to how the entity communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.
3. *Risk assessment:* The criteria relevant to how the entity (i) identifies potential risks that would affect the entity’s ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.

4. *Monitoring activities:* The criteria relevant to how the entity monitors the system, including the suitability and design and operating effectiveness of the controls, and acts to address deficiencies identified.
5. *Control activities:* The criteria relevant to the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.
6. *Logical and physical access controls:* The criteria relevant to how the entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
7. *System operations:* The criteria relevant to how the entity manages the operation of system(s) and detects and mitigates processing deviations, including logical and physical security deviations.
8. *Change management:* The criteria relevant to how the entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
9. *Risk mitigation:* The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

This report is focused solely on the security, availability, and confidentiality categories. The Company has elected to exclude the processing integrity and privacy categories.

Applicable Standards from the HIPAA Security Rule and Breach Notification Rule

The HIPAA Security Rule specifically focuses on the safeguarding of electronic protected health information (ePHI) through the implementation of administrative, physical, and technical safeguards. Compliance is mandated to all organizations defined by HIPAA as a Covered Entity and Business Associate. These organizations are each required to:

- Ensure the confidentiality, integrity, and availability of all ePHI that it creates, receives, maintains, or transmits
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information
- Protect against reasonably anticipated unauthorized uses or disclosures of PHI
- Ensure compliance by its workforce

The requirements of the HIPAA Security Rule are organized according to safeguards, standards, and implementation specifications. The major sections include the following:

- §164.308 Administrative Safeguards
- §164.310 Physical Safeguards
- §164.312 Technical Safeguards
- §164.314 Organizational Requirements
- §164.316 Policies and Procedures
- Documentation Requirements

While the administrative, physical, and technical requirements identified under HIPAA are mandatory, their implementation may differ based on the type of requirement. Under the HIPAA Security Rule, Standards and Implementation Specifications are classified as either “Required” or “Addressable.” It is important to note that neither of these classifications should be interpreted as “optional.” An explanation of each is provided below:

- **Required**: Implementation specifications identified as “required” must be fully implemented by the covered organization. Furthermore, all HIPAA Security and Breach Notification Rules identified as “Standards” are classified as “required.”
- **Addressable**: The concept of an “addressable” implementation specification was developed to provide flexibility to covered organizations with respect to how the requirement could be satisfied. To meet the requirements of an addressable specification, a covered organization must: (a) implement the addressable implementation specification as defined; (b) implement one or more alternative security measures to accomplish the same purpose; or (c) not implement either an addressable implementation specification or an alternative. Where the organization chooses an alternative control or determines that a reasonable and appropriate alternative is not available, the organization must fully document its decision and reasoning. The written documentation should include the factors considered, as well as the results of the risk assessment on which the decision was based.

The HIPAA Breach Notification Rule, 45 CFR §164.404 - 414, requires HIPAA-covered entities and their business associates to provide notification following a breach of unsecured PHI. The major sections of the rule include the following:

- §164.404 Notification to individuals
- §164.406 Notification to the media
- §164.408 Notification to the Secretary
- §164.410 Notification by a business associate
- §164.412 Law enforcement delay
- §164.414 Administrative requirements and burden of proof

Control Environment

Integrity, Ethical Values, and Competence

Integrity, ethical values, and competence are essential components of Atlassian's control environment. All Atlassian employees must acknowledge the Code of Business Conduct and Ethics. The People team is responsible for reviewing and monitoring compliance with these policies and agreements and ensuring that background screening procedures are carried out promptly.

Board of Directors, Audit Committee, and Assignment of Authority and Responsibility

Atlassian's Board of Directors and subcommittees), all of which are part of the Executive Management team, meet annually to review committee charters, corporate governance, and strategic operational objectives. Meeting minutes are recorded with details on participants and dates. Targets are conveyed to product groups for execution by Executive Management, with progress evaluated quarterly. Audit committee information is accessible on Atlassian’s Investor website, including roles, responsibilities, key activities, meetings, qualifications for Financial Expert role, meeting calendar, and agenda developed annually with results published after each meeting.

Board and Governance Committee Charter

The Board of Directors and its subcommittees annually review the Board of Directors charter, Audit committee charter, and the Nominating and Governance committee charter that outline each committee's respective roles, responsibilities, meeting frequency, participants, member qualifications, discussion topics, and key activities. The Nominating and Governance committee charter defines the process of identifying and reviewing candidates for the Board of Directors.

Management's Philosophy and Operating Style

At Atlassian, Executive Management are continuously engaged in a controlled environment. The Risk and Compliance team follows specific standards for security, availability, confidentiality, quality, and reliability. Customized tools assist in identifying risks and findings while workflows ensure proper tracking of activities. An Enterprise Risk Management process modeled after International Organization for Standardization (ISO) 31000:2018 is used to create universal control activities that meet multiple standards. This approach promotes operational efficiency and a unified language across the organization.

Rules of Behavior

Atlassian requires all employees and specified contractors to acknowledge the Code of Business Conduct and Ethics, Insider Trading Policy, Foreign Corrupt Practices Act (FCPA) Agreement, and Anti-Corruption Policy upon hire to ensure that they are aware of their responsibilities and expected behavior. The Code of Business Conduct and Ethics policy is reviewed on an annual basis. Atlassian ensures that all relevant personnel have appropriate access agreements in place.

A hotline for whistleblowers has been established and is available to both external individuals and Atlassian employees. It is included in the Code of Business Conduct and Ethics, which all employees are required to acknowledge. Atlassian adheres to the Policy Violation Investigation Process when conducting investigations that may require disciplinary action, up to and including termination of employment, for individuals who fail to comply. Atlassian also requires its employees to complete anti-harassment training.

Personnel Management and Termination

Background checks are completed for new employees prior to their start date and a weekly review is conducted to confirm that the Confidential Information and Inventions Assignment (CIIA) has been signed as part of the onboarding process. For external candidates, the hiring manager or the People team reviews and formally approves every offer that is made. The Talent Acquisition team approves offers for interns and graduates due to the bulk nature and timing of these hires.

Atlassian has a documented performance review process in place and reviews employee performance on an annual basis. Growth plans are created to help employees understand expected attitudes, behavior, and skills that contribute to success in a role and to connect them to resources aimed at improving those skills. Atlassian provides opportunities for professional development via training or tuition reimbursement and online learning management systems.

Information and Communication

Internal Audit

The Internal Audit team is responsible for carrying out procedures to confirm adherence to and verification with the internal information security management system. The design of controls and mitigation strategies are reviewed on an annual basis. The outcomes of internal audits are documented, and corrective actions are monitored via reports to management.

Awareness and Training

Atlassian delivers annual security awareness training to all employees upon commencement of employment and annually thereafter. This program ensures staff are made aware of security risks and regulations. Automated notification reminders are sent to employees and escalated to their managers to make sure training is completed by the respective deadlines.

Program Management

Atlassian maintains a security policy, which is shared and reviewed annually to ensure that security is appropriately designed and integrated into the system. The policies are posted online, assigned a policy owner, and reviewed at least annually by the designated policy owner or their delegate.

Atlassian has a personnel development program for the security and confidentiality workforce, and training is provided to employees to support their ongoing development and growth. An organizational chart is in place and updated to ensure identification of roles and responsibilities. The organizational chart is reviewed by appropriate Atlassian management and updated as needed.

Atlassian implements a process to ensure that strategic operational objectives are set, reviewed, and properly prioritized. The Executive Management team sets strategic operational objectives quarterly.

System Security Plan

Atlassian provides detailed documentation on system boundaries, product descriptions, and key services on both the Atlassian intranet and customer-facing website. Internal users and customers are informed of significant changes made to key products and features. Atlassian also communicates changes to security, availability and confidentiality commitments on the Atlassian Trust Center. For any material changes, an additional notice is also provided.

Incident Response

Atlassian maintains a company-wide incident management policy that is shared and reviewed on an annual basis. Incident management response procedures and plans are integrated into mission-critical business processes and systems to minimize downtime, service degradation, and security risk for customers and internal users. System availability is published to help users handle and report incidents. Atlassian also provides a variety of methods and channels for customers to report incidents, system vulnerabilities, bugs, and issues related to defects, security, availability, and confidentiality.

Risk Assessment and Mitigation

Enterprise Risk Management

Atlassian's framework for enterprise risk management is developed, documented, and reviewed annually to manage risks related to Atlassian's strategy and business objectives. Atlassian has a Risk Management policy that is shared, assigned a policy owner, and reviewed at least annually by the designated policy owner or their delegate. Atlassian has a risk assessment process in place in which risks are documented with a risk rating and assigned a risk owner. Atlassian ensures that risks outside of the acceptable level of risk are monitored and that risk assessments are reviewed annually.

Fraud Risk Assessments

A fraud risk assessment is performed annually by the Head of Risk and Compliance or a delegate. The assessment includes a cross-functional survey of employees in areas susceptible to fraud combined with an evaluation of external risks. The report results are evaluated and communicated to executive level management and the Audit committee.

Supplier Assessment and Review

Atlassian ensures that its vendors meet security, availability, and confidentiality commitments during the procurement process and on an ongoing basis, as applicable. Atlassian follows a defined process for vendor reviews, which includes an Initial Supplier Risk Assessment, Supplier Due Diligence and Risk Treatment, Contract Management, and Supplier Monitoring. To achieve Atlassian's principal service commitments and system requirements, Atlassian reviews SOC reports at least annually for material third-party services and applications to ensure that controls are appropriate and operating effectively.

Monitoring

Vulnerability Management

Atlassian performs vulnerability scanning on a continuous basis. Atlassian ensures that any legitimate vulnerabilities are remediated in accordance with the vulnerability management policy.

Penetration Testing

Atlassian conducts penetration testing at least annually on all publicly accessible Atlassian products. Bug bounty programs are utilized to detect traditional web application vulnerabilities as well as other vulnerabilities that can have a direct impact. These vulnerabilities are tracked and mitigated until they are resolved.

Control Activities

Access Control

Atlassian ensures that access to services, products, cloud service providers, internal systems, and tools is managed in compliance with relevant access control policies. Access is provisioned in line with the principle of least privilege only after approval is documented via a Jira ticket or in the internal Self Service Access Management (SSAM) tool and is reviewed at least semi-annually.

Registration and de-registration of user access is restricted to authorized users via AD group membership, which is automatically assigned based on the user’s department and team. AD contains a subset of groups that are automatically created and maintained based on demographic and employment information in the Workday system. These groups are based on division, team, location, employment type, and management status. As well as initially provisioning membership, the staff members’ assigned groups are updated to reflect a team or department change or termination.

Automatic alerts are generated for role changes made in reassignment or transfer of personnel. User access to products and services is modified as necessary to correspond to these changes. Atlassian ensures that within 8 hours of a personnel termination, the user’s access is revoked to products, production systems, tools, services, and the network.

Identification and Authentication

Atlassian products and services are secured with passwords and multi-factor authentication (MFA). This ensures that only authorized individuals can access cloud services and remote access systems.

Atlassian employees are uniquely identified and authenticated using AD, which enforces password settings in accordance with the password standard. Atlassian's SSO portal (Idaptive) allows users to have a single point of authentication to access multiple applications.

In cases where MFA is not available, a distinct username and password must be provided. MFA is mandatory to access the virtual private network (VPN) from any IP address and when launching an application from Idaptive.

Customers are uniquely identified and authenticated as well using password mechanisms that are controlled by their Atlassian account. Unless an external identity provider is implemented by the customer, customers must meet the minimum password requirements that are controlled via their Atlassian account.

System Operations

Boundary Protection

Atlassian has firewall rules in place to restrict access to the production environment. The firewalls are configured to limit unnecessary ports, protocols, and services. Atlassian manages and monitors external interfaces and key internal interfaces to the products and services to prevent unauthorized use or access.

Malicious Code Protection

Atlassian implements and enforces malware protection on corporate endpoints. An enterprise anti-malware platform provides endpoint protection, centralized reporting, and notifications. Atlassian quarantines any malicious software upon detection of suspicious activities, and incident tickets are created for review and are resolved in a timely manner.

Mobile Devices

Usage restrictions, configuration/connection requirements, and authorization are documented and established for mobile devices.

Encryption

Atlassian implements cryptographic mechanisms to prevent unauthorized disclosure and modification of data in transit and at rest.

Change Management

Atlassian ensures that configuration-controlled changes to products, services, and the infrastructure are reviewed, approved, and documented. Change management responsibilities are segregated among designated personnel. Emergency changes undergo a similar process. In the event of a catastrophic failure, Atlassian has break glass procedures in place to bypass MFA required for the VPN and the Atlassian SSO (Idaptive) portal.

Configuration changes are documented and monitored for non-compliance. An alert is automatically generated if a change to the peer review enforcement for pull requests occurs.

Prevention of Unauthorized Changes

Atlassian enforces restrictions on infrastructure access to prevent unauthorized modifications. Only artifacts with a valid signature from build software can be released to the production environment. If unauthorized hardware, software, or firmware components are detected, they are isolated, and access is disabled until the relevant support personnel are notified. IT Asset management software is utilized to enforce hard drive encryption, user authentication requirements, and security patching on MacOS and Windows endpoints.

Availability

Contingency Planning and Backups

Atlassian has a disaster recovery policy that has been assigned a policy owner and is reviewed at least annually by the designated policy owner or their delegate. It outlines the purpose, objectives, scope, critical dependencies, recovery time objective/recovery point objective (RTO/RPO), and roles and responsibilities. These details are also available online on the Atlassian Trust Center.

Atlassian conducts quarterly disaster recovery tests are and performs exercises to help disaster response teams walk through various scenarios. Post testing, outputs are captured and analyzed to determine next steps for continued improvement.

Atlassian performs backups at least daily and annual restoration testing of system data for its products and services to ensure that data security, integrity, and reliability are maintained. Capacity management is performed on an ongoing basis by all products. Changes to the availability and processing capacity of the customer-facing service products and key services are internally monitored and adjusted accordingly.

Confidentiality

Information Handling and Retention

Atlassian ensures that customer data is deleted within a reasonable time frame upon request or termination of contract. Upon termination of contract, the customer's account is deactivated after the end of the customer's current subscription period. Atlassian retains data for deactivated products for up to 60 days after the end of the customer's current subscription period. Upon deletion, an archive of the data is kept at a minimum for an additional 30 days.

Access to Customer Data

Customer data is logically isolated using unique identifiers. Access to customer data is granted implicitly through customer support tickets or active incidents. This access is for troubleshooting purposes and is granted via tokens only for a limited period of time or until the incident is closed. Customer support tickets can only be submitted by individuals delegated as administrators within Atlassian Admin.

Complementary User Entity Controls (CUECs)

The Company's controls related to Confluence Databases and Confluence Whiteboards cover only a portion of overall internal control for each user entity of Confluence Databases and Confluence Whiteboards. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls described in Section 4 of this report, considering the related CUECs identified for the specific criterion. For user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls
CC2.1	• User entities are responsible for identifying approved points of contacts to coordinate with Atlassian. • User entities are responsible for the security and confidentiality of the data submitted on Atlassian support tickets.
CC2.3	• User entities are responsible for assessing and evaluating any potential impact that add-ons may have on their instance.
CC6.1	• User entities are responsible for configuring their own instance, including the appropriate setup of their logical security and privacy settings (such as IP allowed listing, 2FA, SSO, password settings, and restricting public access). • User entities are responsible for changing their passwords to reflect a minimum length of at least eight characters where they have migrated from another identity service. • User entities are responsible for safeguarding their own account access credentials, including passwords or application programming interface (API) keys and tokens.
CC6.6 CC6.8 C1.1 C1.2	• User entities are responsible for security, including virus scans and confidentiality of the data (e.g., media attachments), prior to import or attachment and its ongoing monitoring after data has been uploaded.
CC6.2 CC6.3	• User entities are responsible for managing access rights, including privileged access. • Customers are responsible for requesting, approving, and monitoring Atlassian's customer support access to their account.
CC6.2 CC6.3 C1.2	• User entities are responsible for requesting removal of their account.
CC6.6 CC6.7 CC6.8	• User entities are responsible for ensuring that their machines, devices, and network are secured.
CC7.3	• User entities are responsible for alerting Atlassian of incidents (related to security, availability, and confidentiality) when they become aware of them.

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS and Cloudflare as subservice organizations for data center colocation services. The Company's controls related to Confluence Databases and Confluence Whiteboards cover only a portion of the overall internal control for each user entity of Confluence Databases and Confluence Whiteboards. The description does not extend to the colocation services for IT infrastructure provided by the subservice organizations. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of the Company and exclude the related controls of AWS and Cloudflare.

The following table outlines the individual colocation hosting and database hosting services responsibilities of the subservice organizations:

Subservice Organization	Products Applicable to the Subservice Organization
AWS (Data hosting)	Confluence Databases, Confluence Whiteboards
Cloudflare (Temporary data storage and hosting)	Confluence Databases, Confluence Whiteboards

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. CSOCs are expected to be in place at AWS and Cloudflare related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS' and Cloudflare's physical security controls should mitigate the risk of unauthorized access to the hosting facilities. AWS' environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities. In addition, CSOCs are expected to be in place at Cloudflare relating to the encryption of data stores.

The Company management receives and reviews the AWS and Cloudflare SOC 2 reports annually. In addition, through its operational activities, the Company management monitors the services performed by AWS and Cloudflare to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS and Cloudflare management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to Confluence Databases and Confluence Whiteboards to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls described in Section 4 of this report, considering the related CSOCs expected to be implemented at AWS and Cloudflare as described below.

Criteria	Complementary Subservice Organization Controls
CC6.1 CC6.2 CC6.3	• AWS and Cloudflare are responsible for IT access above least privileged, including administrator access. • AWS and Cloudflare are responsible for approval by appropriate personnel prior to access provisioning. • AWS and Cloudflare are responsible for privileged IT access reviews on a regular basis. • AWS and Cloudflare are responsible for timely revocation of user access upon termination. • AWS and Cloudflare are responsible for encrypting data in transit and at rest.
CC6.4	• AWS and Cloudflare are responsible for restricting physical access to the computer rooms that house the entity's IT resources, servers, and related hardware to authorized individuals through a badge access system or equivalent that is monitored by video surveillance. • AWS and Cloudflare are responsible for approving requests for physical access privileges from an authorized individual. • AWS and Cloudflare are responsible for requiring visitors to be signed in by an authorized workforce member before gaining entry and for always escorting approved visitors.
CC6.5 CC6.7	• AWS and Cloudflare are responsible for securely decommissioning and physically destroying production assets in their control.

Criteria	Complementary Subservice Organization Controls
CC7.1 CC7.2 CC7.3	• AWS and Cloudflare are responsible for implementing and monitoring electronic intrusion detection systems that can detect breaches into data center server locations. • AWS and Cloudflare are responsible for documenting procedures for the identification and escalation of potential security breaches.
CC7.2 A1.2	• AWS and Cloudflare are responsible for installing environmental protection that includes the following: cooling systems, battery and generator backups, smoke detection, and dry pipe sprinklers. • AWS and Cloudflare are responsible for monitoring the environmental protection equipment for incidents or events that impact assets.
CC8.1	• AWS and Cloudflare are responsible for ensuring that changes are authorized, tested, and approved prior to implementation.

Specific Criteria Not Relevant to the System

There were no specific security, availability, or confidentiality Trust Services Criteria as set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (With Revised Points of Focus—2022)* (2017 TSC) that were not relevant to the system as presented in this report.

Atlassian has determined that the following HIPAA Security and Breach Notification Rules are not relevant to the system:

- § 164.308(a)(4)(ii)(A) is not relevant because Atlassian does not function as a health care clearinghouse.
- § 164.308(b)(1), § 164.314(a)(2)(ii), § 164.404(a) - § 164.408(c), and § 164.414(a) are not relevant because Atlassian is not a covered entity.
- § 164.314(b) is not relevant because Atlassian is not a group health plan.

Report Use

The description does not omit or distort information relevant to Confluence Databases and Confluence Whiteboards while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to their own needs.

Section 4

Trust Services Criteria and Related Controls Relevant to the Security, Availability, and Confidentiality Categories and HIPAA Security and Breach Notification Rules

Trust Services Criteria and Related Controls Relevant to the Security, Availability, and Confidentiality Categories

Control Environment	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
CC1.1	The entity demonstrates a commitment to integrity and ethical values.
	A comprehensive Code of Business Conduct and Ethics describes employee and contractor responsibilities and expected behavior regarding data and information system usage. The policy is shared and reviewed annually.
	Employees acknowledge the Code of Business Conduct and Ethics policy upon hire.
	Employee performance is reviewed annually.
	The Company has documented disciplinary actions in a formalized sanctions policy for employees and contractors who violate the Code of Business Conduct and Ethics.
	Background checks are performed prior to an employee's start date in compliance with local laws and regulations.
	Employees are required to sign Confidential Information and Inventions Assignments (CIIAs) as part of the onboarding process.
	A weekly review is performed to determine whether the CIIA and background checks are completed for new employees as part of onboarding procedures.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
	The Board and Committee Charter outlines the roles, responsibilities, and key activities of the board.
	The Audit Committee Charter outlines the roles, responsibilities, and key activities of the Audit Committee.
	Atlassian's Board of Directors and subcommittees meet annually to review committee charters, corporate governance, and strategic operational objectives. Meeting minutes are recorded with details on participants and dates.
	The Nominating and Governance Committee Charter clearly outlines the roles, responsibilities, and key activities of the Nominating and Governance Committee.

Control Environment	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
	An organizational chart is in place and updated to ensure identification of roles and responsibilities.
	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment including compliance with HIPAA.
	The hiring manager reviews and approves employee job descriptions.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
	Employees are required to complete security awareness training upon hire and at least annually thereafter.
	A personnel development program for security and confidentiality has been established.
	The hiring manager reviews and approves employee job descriptions.
	Employee performance is reviewed annually.
	External candidates are formally approved prior to receiving an offer.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
	Employee performance is reviewed annually.
	A comprehensive Code of Business Conduct and Ethics describes employee and contractor responsibilities and expected behavior regarding data and information system usage. The policy is shared and reviewed annually.
	Employees acknowledge the Code of Business Conduct and Ethics policy upon hire.
	The Company has documented disciplinary actions in a formalized sanctions policy for employees and contractors who violate the Code of Business Conduct and Ethics.
	The hiring manager reviews and approves employee job descriptions.

Information and Communication	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
	Internal audits are performed annually, results are communicated to management and the Audit Committee, and corrective actions are monitored.
	Vulnerability scanning is performed continuously.
	Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy.
	A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when specific events occur.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
	Employees are required to complete security awareness training upon hire and at least annually thereafter.
	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment including compliance with HIPAA.
	The hiring manager reviews and approves employee job descriptions.
	A whistleblower process is established and accessible to both external individuals and employees.
	The Executive Team reviews, sets, and/or revises strategic operational objectives quarterly. The targets are cascaded down into each of the product groups for execution by the Management Team.
	System boundaries, product descriptions, and key services are documented in detail on both the Atlassian intranet and the customer-facing website.
	Significant changes made to key products and services are communicated to internal users and customers.

Information and Communication	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.
	The Atlassian Customer Agreement and product-specific ToS communicate Atlassian's commitments and the customer responsibilities. The ToS are published on the Atlassian customer-facing website, and any changes are communicated.
	Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed during the procurement process for all critical vendors.
	Significant changes made to key products and services are communicated to internal users and customers.
	Users may report bugs; defects; or availability, security, and confidentiality issues.
	System availability is published to provide assistance to users for the handling and reporting of incidents.
	Atlassian communicates changes to security, availability, and confidentiality commitments.

Risk Assessment	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
	The design of controls and mitigation strategies are reviewed annually, including identifying risks and recommending changes in the control environment.
	A Risk Management policy is made available to employees and reviewed annually.
	Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
	A Risk Management policy is made available to employees and reviewed annually.
	Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders.
	A fraud risk assessment is performed annually by the Head of Risk and Compliance or delegate. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. The report results are evaluated and included within the enterprise risk assessment, which is communicated to the board and executive-level managers annually.
	A disaster recovery policy is shared on the Company intranet and reviewed annually.
	A disaster recovery plan is in place and tested quarterly.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.
	A Risk Management policy is made available to employees and reviewed annually.
	Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders.

Risk Assessment	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
	A fraud risk assessment is performed annually by the Head of Risk and Compliance or delegate. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. The report results are evaluated and included within the enterprise risk assessment, which is communicated to the board and executive-level managers annually.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.
	A Risk Management policy is made available to employees and reviewed annually.
	Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders.
	A fraud risk assessment is performed annually by the Head of Risk and Compliance or delegate. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. The report results are evaluated and included within the enterprise risk assessment, which is communicated to the board and executive-level managers annually.
	Penetration testing is performed at least annually.
	Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy.

Monitoring Activities	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
	Internal audits are performed annually, results are communicated to management and the Audit Committee, and corrective actions are monitored.
	Penetration testing is performed at least annually.
	Vulnerability scanning is performed continuously.
	Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy.
	SOC 2 reports of critical vendors are reviewed annually.
	Suppliers who host or process data undergo an assessment to ensure security, availability, and confidentiality requirements are met.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
	Internal audits are performed annually, results are communicated to management and the Audit Committee, and corrective actions are monitored.
	SOC 2 reports of critical vendors are reviewed annually.
	Suppliers who host or process data undergo an assessment to ensure security, availability, and confidentiality requirements are met.

Control Activities	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
	The design of controls and mitigation strategies are reviewed annually, including identifying risks and recommending changes in the control environment.
	Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.
	The design of controls and mitigation strategies are reviewed annually, including identifying risks and recommending changes in the control environment.
	Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
	Formal procedures are documented that outline the process the Company's staff follows to perform the following system access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access - Restricting access based on separation of duties and least privilege
	A security policy is shared on the Company intranet and reviewed annually.
	All policies are posted and available and reviewed at least annually.
	A Risk Management policy is made available to employees and reviewed annually.
	Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data.
	A data classification policy is in place to support the safety and security of data Atlassian holds.

Control Activities	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
	Formal procedures are documented that outline requirements for vulnerability management and system monitoring. The procedures are reviewed at least annually.
	A vendor management program is in place. Components of this program include: - Maintaining a list of critical vendors - Requirements for critical vendors to maintain their own security practices and procedures - Annually reviewing attestation reports for critical vendors or performing a vendor risk assessment
	A formal systems development life cycle (SDLC) methodology is in place that governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements.
	Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data, and requires HIPAA related documentation to be retained for at least 6 years.
	An incident management policy is shared on the Company intranet and reviewed annually.

Logical and Physical Access Controls	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	Customers are uniquely identified and authenticated via unique identifiers.
	Two-factor authentication is required when logging into the virtual private network (VPN - Remote Access Service) from any internet protocol (IP) address.
	Two-factor authentication is required when launching an application from the SSO system (Idaptive).
	Passwords for in-scope system components are configured according to the Company's policy, which requires the following (unless there is a system limitation): - 8 character minimum - Lockout after 5 invalid attempts The password policy addresses how and when users should change their passwords.
	Active Directory (AD) enforces password settings in line with the Atlassian Password Standard. Idaptive Single Sign On (SSO) allows users to have a single point of authentication to access multiple applications. Password settings for Idaptive are enforced by AD via the AD connector for Idaptive.
	A formal inventory of production system assets that includes asset owners is maintained, and changes to the inventory are logged.
	Customer data is logically isolated through the use of unique identifiers.
	A Zero Trust infrastructure is implemented to place endpoints into a tiered network (High, Low, Open) based on their security posture and type of device. Applications added to the SSO platform are tiered according to the Zero Trust policy. Endpoints cannot access applications via the SSO platform unless they are placed on the same/higher tier as the application.
	Cryptographic mechanisms are implemented or enabled to prevent unauthorized disclosure and modification of data at rest.

Logical and Physical Access Controls	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	Access to customer data requires a valid customer support request or the existence of an active incident that requires access to be resolved.
	AD accounts and permissions are automatically assigned based on user descriptions associated with Workday.
	The provisioning of service and product accounts is based on job role and function and requires manager approval prior to access being provisioned.
	AD accounts and network access are automatically disabled within 8 hours from the time an employee is marked as terminated in the HR system.
	The HR system does not allow terminations to be backdated.
	Access to internal systems and tools is reviewed at least semi-annually, and issues identified are remediated in a timely manner.
	Access to products and services is reviewed at least semi-annually, and issues identified are remediated in a timely manner.
	Access to the Atlassian internal network and internal tools is restricted to authorized users via the following logical access measures: - Each user account must have an active AD account - Each user account must be a member of the appropriate AD group
	An automatic alert is sent for any role change between the following groups: Engineering, Customer Support & Success (CSS), or Finance group. Appropriateness of access is reviewed and approved.

Logical and Physical Access Controls	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
	Access to customer data requires a valid customer support request or the existence of an active incident that requires access to be resolved.
	Privileged access for products and services, including access to migrate to production, is restricted based on job description.
	Privileged access to internal systems and tools, including access to migrate to production, is restricted based on job description.
	Access to the Atlassian internal network and internal tools is restricted to authorized users via the following logical access measures: - Each user account must have an active AD account - Each user account must be a member of the appropriate AD group
	Only service owners can assign delegates to key infrastructure and services.
	An automatic alert is sent for any role change between the following groups: Engineering, Customer Support & Success (CSS), or Finance group. Appropriateness of access is reviewed and approved.
	AD accounts and permissions are automatically assigned based on user descriptions associated with Workday.
	The provisioning of service and product accounts is based on job role and function and requires manager approval prior to access being provisioned.
	AD accounts and network access are automatically disabled within 8 hours from the time an employee is marked as terminated in the HR system.
	Access to internal systems and tools is reviewed at least semi-annually, and issues identified are remediated in a timely manner.
	Access to products and services is reviewed at least semi-annually, and issues identified are remediated in a timely manner.
	Multi-factor authentication is used for privileged accounts unless there is a system limitation.

Logical and Physical Access Controls	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
	The Company's production environment is hosted at third-party data centers, which are carved out for the purposes of this report.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
	A formal inventory of production system assets that includes asset owners is maintained, and changes to the inventory are logged.
	Storage media containing sensitive data and licensed software is removed and securely overwritten prior to disposal.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
	Multi-factor authentication is used for privileged accounts unless there is a system limitation.
	Two-factor authentication is required when logging into the virtual private network (VPN - Remote Access Service) from any internet protocol (IP) address.
	Two-factor authentication is required when launching an application from the SSO system (Idaptive).
	External interfaces to the products and services and key internal interfaces are managed and monitored to prevent unauthorized use or access.
	External interfaces to the infrastructure and shared services and key internal interfaces are managed and monitored to prevent unauthorized use or access.
	Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
	IT asset management software is used to enforce hard drive encryption, user authentication requirements, usage restrictions, authorizations and security patching on Mac/Windows endpoints.

Logical and Physical Access Controls	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
	IT asset management software is used to enforce hard drive encryption, user authentication requirements, usage restrictions, authorizations and security patching on Mac/Windows endpoints.
	Cryptographic mechanisms are implemented to prevent unauthorized disclosure and modification of data in transit.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
	Malicious code protection is implemented on endpoints and servers.
	External interfaces to the products and services and key internal interfaces are managed and monitored to prevent unauthorized use or access.
	External interfaces to the infrastructure and shared services and key internal interfaces are managed and monitored to prevent unauthorized use or access.
	A Zero Trust infrastructure is implemented to place endpoints into a tiered network (High, Low, Open) based on their security posture and type of device. Applications added to the SSO platform are tiered according to the Zero Trust policy. Endpoints cannot access applications via the SSO platform unless they are placed on the same/higher tier as the application.

System Operations	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
	Vulnerability scanning is performed continuously.
	Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy.
	Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
	A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when specific events occur.
	Vulnerability scanning is performed continuously.
	Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy.
	Penetration testing is performed at least annually.
	The availability and capacity of each service and its underlying infrastructure are monitored continuously through the use of monitoring tools. Alerts are automatically sent to on-call engineers when early warning thresholds are crossed on key operational metrics.

System Operations	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
	Security events are reviewed and handled in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems, which includes the evaluation, logging, tracking, and communication of all events.
	Penetration testing is performed at least annually.
	Vulnerability scanning is performed continuously.
	Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy.
	An incident management policy is shared on the Company intranet and reviewed annually.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
	Security incidents are reviewed and handled in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems, which includes the evaluation, logging, tracking, and communication of all incidents.
	An incident management policy is shared on the Company intranet and reviewed annually.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.
	A disaster recovery policy is shared on the Company intranet and reviewed annually.
	A disaster recovery plan is in place and tested quarterly.
	An incident management policy is shared on the Company intranet and reviewed annually.
	Security incidents are reviewed and handled in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems, which includes the evaluation, logging, tracking, and communication of all incidents.

Change Management	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
	Configuration-controlled changes to infrastructure are tested, reviewed, approved, and documented.
	Configuration-controlled changes to products and services are tested, reviewed, and approved. Change management responsibilities are segregated among designated personnel.
	Configuration changes are documented and monitored for non-compliance. An alert is automatically generated if a change to the peer review enforcement for pull requests occurs.
	Infrastructure access restrictions are configured to prevent unauthorized changes.
	Privileged access to internal systems and tools, including access to migrate to production, is restricted based on job description.

Risk Mitigation	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
	A Risk Management policy is made available to employees and reviewed annually.
	A disaster recovery policy is shared on the Company intranet and reviewed annually.
	A disaster recovery plan is in place and tested quarterly.
	An incident management policy is shared on the Company intranet and reviewed annually.
	A multi-location strategy is employed for production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility.
	Databases are replicated to secondary availability zones in real time. Alerts are configured to notify administrators if replication fails.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.
	SOC 2 reports of critical vendors are reviewed annually.
	Suppliers who host or process data undergo an assessment to ensure security, availability, and confidentiality requirements are met.
	Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed during the procurement process for all critical vendors.

Additional Criteria for Availability

Availability	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
	System availability is published to provide assistance to users for the handling and reporting of incidents.
	The availability and capacity of each service and its underlying infrastructure are monitored continuously through the use of monitoring tools. Alerts are automatically sent to on-call engineers when early warning thresholds are crossed on key operational metrics.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.
	A disaster recovery policy is shared on the Company intranet and reviewed annually.
	A disaster recovery plan is in place and tested quarterly.
	System data of products and services is backed up at least daily. Restoration testing occurs annually to ensure data security and integrity is maintained.
	A multi-location strategy is employed for production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility.
	Databases are replicated to secondary availability zones in real time. Alerts are configured to notify administrators if replication fails.
	Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.
	A disaster recovery policy is shared on the Company intranet and reviewed annually.
	A disaster recovery plan is in place and tested quarterly.
	Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data.
	System data of products and services is backed up at least daily. Restoration testing occurs annually to ensure data security and integrity is maintained.

Additional Criteria for Confidentiality

Confidentiality	
TSC Reference	**Trust Services Criteria and Applicable Control Activities**
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
	A data classification policy is in place to support the safety and security of data Atlassian holds.
	Production data is not used in non-production environments as part of the Software Development Lifecycle Procedures.
	Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed during the procurement process for all critical vendors.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.
	Customer data is disposed of, destroyed, or erased upon request in accordance with the retention period or upon termination of services.
	Storage media containing sensitive data and licensed software is removed and securely overwritten prior to disposal.

HIPAA Security and Breach Notification Rules

Administrative Safeguards – §164.308			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Security Management Process	§ 164.308(a)(1)(i)	Implement policies and procedures to prevent, detect, contain, and correct security violations.	A security policy is shared on the Company intranet and reviewed annually.
			Penetration testing is performed at least annually.
			Vulnerability scanning is performed continuously.
			Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy.
Risk Analysis	§ 164.308(a)(1)(ii)(A)	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.	Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders.
			Internal audits are performed annually, results are communicated to management and the Audit Committee, and corrective actions are monitored.
			A Risk Management policy is made available to employees and reviewed annually.

Administrative Safeguards – §164.308			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
			A fraud risk assessment is performed annually by the Head of Risk and Compliance or delegate. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. The report results are evaluated and included within the enterprise risk assessment, which is communicated to the board and executive-level managers annually.
Risk Management	§ 164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	The Executive Team reviews, sets, and/or revises strategic operational objectives quarterly. The targets are cascaded down into each of the product groups for execution by the Management Team.
			Internal audits are performed annually, results are communicated to management and the Audit Committee, and corrective actions are monitored.
			A Risk Management policy is made available to employees and reviewed annually.
			A fraud risk assessment is performed annually by the Head of Risk and Compliance or delegate. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. The report results are evaluated and included within the enterprise risk assessment, which is communicated to the board and executive-level managers annually.

Administrative Safeguards – §164.308			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
			Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders.
Sanction Policy	§ 164.308(a)(1)(ii)(C)	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	The Company has documented disciplinary actions in a formalized sanctions policy for employees and contractors who violate the Code of Business Conduct and Ethics.
Information System Activity Review	§ 164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when specific events occur.
			Access to internal systems and tools is reviewed at least semi-annually, and issues identified are remediated in a timely manner.
			Access to products and services is reviewed at least semi-annually, and issues identified are remediated in a timely manner.
			Security events are reviewed and handled in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems, which includes the evaluation, logging, tracking, and communication of all events.

Administrative Safeguards – §164.308			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
			Security incidents are reviewed and handled in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems, which includes the evaluation, logging, tracking, and communication of all incidents.
Assigned Security Responsibility	§ 164.308(a)(2)	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment including compliance with HIPAA.
Workforce Security	§ 164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph(a)(4) of this section, and to prevent those workforce members who do not have access under paragraph(a)(4) of this section from obtaining access to electronic protected health information.	Formal procedures are documented that outline the process the Company's staff follows to perform the following system access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access - Restricting access based on separation of duties and least privilege
			The provisioning of service and product accounts is based on job role and function and requires manager approval prior to access being provisioned.
			Access to internal systems and tools is reviewed at least semi-annually, and issues identified are remediated in a timely manner.

Administrative Safeguards – §164.308			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
			Access to products and services is reviewed at least semi-annually, and issues identified are remediated in a timely manner.
Authorization and/or Supervision	§ 164.308(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	Formal procedures are documented that outline the process the Company's staff follows to perform the following system access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access - Restricting access based on separation of duties and least privilege
			The provisioning of service and product accounts is based on job role and function and requires manager approval prior to access being provisioned.
			Access to internal systems and tools is reviewed at least semi-annually, and issues identified are remediated in a timely manner.
			Access to products and services is reviewed at least semi-annually, and issues identified are remediated in a timely manner.

Administrative Safeguards – §164.308			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Workforce Clearance Procedure	§ 164.308(a)(3)(ii)(B)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Formal procedures are documented that outline the process the Company's staff follows to perform the following system access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access - Restricting access based on separation of duties and least privilege
			The provisioning of service and product accounts is based on job role and function and requires manager approval prior to access being provisioned.
			Access to internal systems and tools is reviewed at least semi-annually, and issues identified are remediated in a timely manner.
			Access to products and services is reviewed at least semi-annually, and issues identified are remediated in a timely manner.
			Background checks are performed prior to an employee’s start date in compliance with local laws and regulations.

Administrative Safeguards – §164.308			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Termination Procedures	§ 164.308(a)(3)(ii)(C)	Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	Active Directory (AD) accounts and network access are automatically disabled within 8 hours from the time an employee is marked as terminated in the HR system. The HR system does not allow terminations to be backdated.
Information Access Management	§ 164.308(a)(4)(i)	Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of § 164.308(a)(4)(i)	Formal procedures are documented that outline the process the Company's staff follows to perform the following system access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access - Restricting access based on separation of duties and least privilege The provisioning of service and product accounts is based on job role and function and requires manager approval prior to access being provisioned.
Isolating Health Care Clearinghouse Functions	§ 164.308(a)(4)(ii)(A)	164.308(a)(4)(ii)(A) is not relevant because Atlassian does not function as a health care clearinghouse.	Not applicable.

Administrative Safeguards – §164.308			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Access Authorization	§ 164.308(a)(4)(ii)(B)	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	Formal procedures are documented that outline the process the Company's staff follows to perform the following system access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access - Restricting access based on separation of duties and least privilege
			The provisioning of service and product accounts is based on job role and function and requires manager approval prior to access being provisioned.
Access Establishment and Modification	§ 164.308(a)(4)(ii)(C)	Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Formal procedures are documented that outline the process the Company's staff follows to perform the following system access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access - Restricting access based on separation of duties and least privilege
			The provisioning of service and product accounts is based on job role and function and requires manager approval prior to access being provisioned.

Administrative Safeguards – §164.308			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
			AD accounts and network access are automatically disabled within 8 hours from the time an employee is marked as terminated in the HR system.
			The HR system does not allow terminations to be backdated.
			Access to internal systems and tools is reviewed at least semi-annually, and issues identified are remediated in a timely manner.
			Access to products and services is reviewed at least semi-annually, and issues identified are remediated in a timely manner.
Security Awareness and Training	§ 164.308(a)(5)(i)	Implement a security awareness and training program for all members of its workforce (including management).	Employees are required to complete security awareness training upon hire and at least annually thereafter.
Security Reminders	§ 164.308(a)(5)(ii)(A)	Periodic security updates.	Employees are required to complete security awareness training upon hire and at least annually thereafter.
			A personnel development program for security and confidentiality has been established.
Protection from Malicious Software	§ 164.308(a)(5)(ii)(B)	Procedures for guarding against, detecting, and reporting malicious software.	Malicious code protection is implemented on endpoints and servers.

Administrative Safeguards – §164.308			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
			Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
			Employees are required to complete security awareness training upon hire and at least annually thereafter.
Log-in Monitoring	§ 164.308(a)(5)(ii)(C)	Procedures for monitoring log-in attempts and reporting discrepancies.	A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when specific events occur.
			Security events are reviewed and handled in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems, which includes the evaluation, logging, tracking, and communication of all events.
			Security incidents are reviewed and handled in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems, which includes the evaluation, logging, tracking, and communication of all incidents.

Administrative Safeguards – §164.308			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Password Management	§ 164.308(a)(5)(ii)(D)	Procedures for creating, changing, and safeguarding passwords.	Passwords for in-scope system components are configured according to the Company's policy, which requires the following (unless there is a system limitation): - 8 character minimum - Lockout after 5 invalid attempts The password policy addresses how and when users should change their passwords.
			Active Directory (AD) enforces password settings in line with the Atlassian Password Standard. Idaptive Single Sign On (SSO) allows users to have a single point of authentication to access multiple applications. Password settings for Idaptive are enforced by AD via the AD connector for Idaptive.
Security Incident Procedures	§ 164.308(a)(6)(i)	Implement policies and procedures to address security incidents.	An incident management policy is shared on the Company intranet and reviewed annually.
			Security incidents are reviewed and handled in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems, which includes the evaluation, logging, tracking, and communication of all incidents.
			Security events are reviewed and handled in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems, which includes the evaluation, logging, tracking, and communication of all events.

Administrative Safeguards – §164.308			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Response and Reporting	§ 164.308(a)(6)(ii)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	An incident management policy is shared on the Company intranet and reviewed annually.
			Employees are required to complete security awareness training upon hire and at least annually thereafter.
			Security incidents are reviewed and handled in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems, which includes the evaluation, logging, tracking, and communication of all incidents.
			Security events are reviewed and handled in accordance with Incident Management procedures and plans to support Atlassian mission and business processes and systems, which includes the evaluation, logging, tracking, and communication of all events.
Contingency Plan	§ 164.308(a)(7)(i)	Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	A disaster recovery policy is shared on the Company intranet and reviewed annually.
			A disaster recovery plan is in place and tested quarterly.
Data Backup Plan	§ 164.308(a)(7)(ii)(A)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	Databases are replicated to secondary availability zones in real time. Alerts are configured to notify administrators if replication fails.

Administrative Safeguards – §164.308			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
			System data of products and services is backed up at least daily. Restoration testing occurs annually to ensure data security and integrity is maintained.
			Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data.
Disaster Recovery Plan	§ 164.308(a)(7)(ii)(B)	Establish (and implement as needed) procedures to restore any loss of data.	A disaster recovery policy is shared on the Company intranet and reviewed annually.
			A disaster recovery plan is in place and tested quarterly.
			Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data.
			Databases are replicated to secondary availability zones in real time. Alerts are configured to notify administrators if replication fails.
			A multi-location strategy is employed for production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility.
			System data of products and services is backed up at least daily. Restoration testing occurs annually to ensure data security and integrity is maintained.

Administrative Safeguards – §164.308			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Emergency Mode Operation Plan	§ 164.308(a)(7)(ii)(C)	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	A disaster recovery policy is shared on the Company intranet and reviewed annually.
			A disaster recovery plan is in place and tested quarterly.
Testing and Revision Procedures	§ 164.308(a)(7)(ii)(D)	Implement procedures for periodic testing and revision of contingency plans.	A disaster recovery policy is shared on the Company intranet and reviewed annually.
			A disaster recovery plan is in place and tested quarterly.
			System data of products and services is backed up at least daily. Restoration testing occurs annually to ensure data security and integrity is maintained.
Applications and Data Criticality Analysis	§ 164.308(a)(7)(ii)(E)	Assess the relative criticality of specific applications and data in support of other contingency plan components.	Services and applications in scope for HIPAA are reviewed annually to determine if their current criticality tier is accurate and aligns with definitions per the business continuity and disaster recovery policy.
Evaluation	§ 164.308(a)(8)	Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	Significant changes made to key products and services are communicated to internal users and customers.
			Vulnerability scanning is performed continuously.
			Vulnerabilities identified in the vulnerability scans and penetration testing are remediated in accordance with the threat and vulnerability management policy.

Administrative Safeguards – §164.308			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
			Penetration testing is performed at least annually.
			Atlassian has defined an Enterprise Risk Management (ERM) process and conducts an enterprise risk assessment annually, which includes key product stakeholders.
			A fraud risk assessment is performed annually by the Head of Risk and Compliance or delegate. A cross-functional survey of employees in areas susceptible to fraud is conducted and combined with an evaluation of external risks. The report results are evaluated and included within the enterprise risk assessment, which is communicated to the board and executive-level managers annually.
			Internal audits are performed annually, results are communicated to management and the Audit Committee, and corrective actions are monitored.
			The design of controls and mitigation strategies are reviewed annually, including identifying risks and recommending changes in the control environment.
Business Associate Contracts and Other Arrangements	§ 164.308(b)(1)	Section 164.308(b)(1) is not relevant because Atlassian is not a covered entity.	Not applicable.

Administrative Safeguards – §164.308			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Business Associate Contracts and Other Arrangements	§ 164.308(b)(2)	A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.	Atlassian obtains satisfactory assurances, in accordance with § 164.314(a), that the company will appropriately safeguard the information if Atlassian creates, receives, maintains, or transmits electronic protected health information on any customer's behalf. These assurances are captured in Business Associate Agreements.
Written Contract or Other Arrangement	§ 164.308(b)(3)	Document the satisfactory assurances required by paragraph(b)(1) or(b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).	Atlassian obtains satisfactory assurances, in accordance with § 164.314(a), that the company will appropriately safeguard the information if Atlassian creates, receives, maintains, or transmits electronic protected health information on any customer's behalf. These assurances are captured in Business Associate Agreements.
			Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed during the procurement process for all critical vendors.

Physical Safeguards – §164.310			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Facility Access Controls	§ 164.310(a)(1)	Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	The Company's production environment is hosted at third-party data centers, which are carved out for the purposes of this report.
Contingency Operations	§ 164.310(a)(2)(i)	Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	A disaster recovery policy is shared on the Company intranet and reviewed annually. A disaster recovery plan is in place and tested quarterly.
Facility Security Plan	§ 164.310(a)(2)(ii)	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	The Company's production environment is hosted at third-party data centers, which are carved out for the purposes of this report.
Access Control and Validation Procedures	§ 164.310(a)(2)(iii)	Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	The Company's production environment is hosted at third-party data centers, which are carved out for the purposes of this report.
Maintenance Records	§ 164.310(a)(2)(iv)	Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	The Company's production environment is hosted at third-party data centers, which are carved out for the purposes of this report.
Workstation Use	§ 164.310(b)	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	A security policy is shared on the Company intranet and reviewed annually. A comprehensive Code of Business Conduct and Ethics describes employee and contractor responsibilities and expected behavior regarding data and information system usage. The policy is shared and reviewed annually.

Physical Safeguards – §164.310			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
			Employees acknowledge the Code of Business Conduct and Ethics policy upon hire.
			Employees are required to sign Confidential Information and Inventions Assignments (CIIAs) as part of the onboarding process.
			A formal inventory of production system assets that includes asset owners is maintained, and changes to the inventory are logged.
Workstation Security	§ 164.310(c)	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	Malicious code protection is implemented on endpoints and servers.
			IT asset management software is used to enforce hard drive encryption, user authentication requirements, usage restrictions, authorizations and security patching on Mac/Windows endpoints.
			Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
			Storage media containing sensitive data and licensed software is removed and securely overwritten prior to disposal.

Physical Safeguards – §164.310			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Device and Media Controls	§ 164.310(d)(1)	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	A formal inventory of production system assets that includes asset owners is maintained, and changes to the inventory are logged.
			Customer data is disposed of, destroyed, or erased upon request in accordance with the retention period or upon termination of services.
			IT asset management software is used to enforce hard drive encryption, user authentication requirements, usage restrictions, authorizations and security patching on Mac/Windows endpoints.
			Storage media containing sensitive data and licensed software is removed and securely overwritten prior to disposal.
Disposal	§ 164.310(d)(2)(i)	Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	Storage media containing sensitive data and licensed software is removed and securely overwritten prior to disposal.
			Customer data is disposed of, destroyed, or erased upon request in accordance with the retention period or upon termination of services.
			Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data, and requires HIPAA related documentation to be retained for at least 6 years.

Physical Safeguards – §164.310			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
			IT asset management software is used to enforce hard drive encryption, user authentication requirements, usage restrictions, authorizations and security patching on Mac/Windows endpoints.
Media Re-Use	§ 164.310(d)(2)(ii)	Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	Storage media containing sensitive data and licensed software is removed and securely overwritten prior to disposal.
			Customer data is disposed of, destroyed, or erased upon request in accordance with the retention period or upon termination of services.
			Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data, and requires HIPAA related documentation to be retained for at least 6 years.
Accountability	§ 164.310(d)(2)(iii)	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	A formal inventory of production system assets that includes asset owners is maintained, and changes to the inventory are logged.
			IT asset management software is used to enforce hard drive encryption, user authentication requirements, usage restrictions, authorizations and security patching on Mac/Windows endpoints.
Data Backup and Storage	§ 164.310(d)(2)(iv)	Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	Formal procedures are documented that outline the process the Company's staff follows to back up and recover customer data.

Physical Safeguards – §164.310			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
			System data of products and services is backed up at least daily. Restoration testing occurs annually to ensure data security and integrity is maintained.
			A disaster recovery policy is shared on the Company intranet and reviewed annually.
			A disaster recovery plan is in place and tested quarterly.

Technical Safeguards – §164.312			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Access Control	§ 164.312(a)(1)	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Formal procedures are documented that outline the process the Company's staff follows to perform the following system access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access - Restricting access based on separation of duties and least privilege
			AD accounts and permissions are automatically assigned based on user descriptions associated with Workday.
			The provisioning of service and product accounts is based on job role and function and requires manager approval prior to access being provisioned.
			AD accounts and network access are automatically disabled within 8 hours from the time an employee is marked as terminated in the HR system.
			The HR system does not allow terminations to be backdated.
			Access to internal systems and tools is reviewed at least semi-annually, and issues identified are remediated in a timely manner.

Technical Safeguards – §164.312			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
			Access to products and services is reviewed at least semi-annually, and issues identified are remediated in a timely manner.
			Active Directory (AD) enforces password settings in line with the Atlassian Password Standard. Idaptive Single Sign On (SSO) allows users to have a single point of authentication to access multiple applications. Password settings for Idaptive are enforced by AD via the AD connector for Idaptive.
			Two-factor authentication is required when logging into the virtual private network (VPN - Remote Access Service) from any internet protocol (IP) address.
			Two-factor authentication is required when launching an application from the SSO system (Idaptive).
			Multi-factor authentication is used for privileged accounts unless there is a system limitation.
Unique User Identification	§ 164.312(a)(2)(i)	Assign a unique name and/or number for identifying and tracking user identity.	Formal procedures are documented that outline the process the Company's staff follows to perform the following system access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access - Restricting access based on separation of duties and least privilege

Technical Safeguards – §164.312			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
			The provisioning of service and product accounts is based on job role and function and requires manager approval prior to access being provisioned.
			Two-factor authentication is required when logging into the virtual private network (VPN - Remote Access Service) from any internet protocol (IP) address.
			Two-factor authentication is required when launching an application from the SSO system (Idaptive).
			Multi-factor authentication is used for privileged accounts unless there is a system limitation.
Emergency Access Procedure	§ 164.312(a)(2)(ii)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	A disaster recovery policy is shared on the Company intranet and reviewed annually.
			A disaster recovery plan is in place and tested quarterly.
Automatic Logoff	§ 164.312(a)(2)(iii)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Sessions are terminated after a specified period for HIPAA in-scope systems.
Encryption and Decryption	§ 164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.	Cryptographic mechanisms are implemented or enabled to prevent unauthorized disclosure and modification of data at rest.

Technical Safeguards – §164.312			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
			Cryptographic mechanisms are implemented to prevent unauthorized disclosure and modification of data in transit.
			IT asset management software is used to enforce hard drive encryption, user authentication requirements, usage restrictions, authorizations and security patching on Mac/Windows endpoints.
Audit Controls	§ 164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	A log management tool is utilized to identify trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when specific events occur.
			Infrastructure supporting the service is patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
			Malicious code protection is implemented on endpoints and servers.
Integrity	§ 164.312(c)(1)	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Cryptographic mechanisms are implemented or enabled to prevent unauthorized disclosure and modification of data at rest.
			Multi-factor authentication is used for privileged accounts unless there is a system limitation.

Technical Safeguards – §164.312			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
			Cryptographic mechanisms are implemented to prevent unauthorized disclosure and modification of data in transit.
Mechanism to Authenticate Electronic Protected Health Information	§ 164.312(c)(2)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	Customer data is logically isolated through the use of unique identifiers.
			External interfaces to the products and services and key internal interfaces are managed and monitored to prevent unauthorized use or access.
			External interfaces to the infrastructure and shared services and key internal interfaces are managed and monitored to prevent unauthorized use or access.
			A Zero Trust infrastructure is implemented to place endpoints into a tiered network (High, Low, Open) based on their security posture and type of device. Applications added to the SSO platform are tiered according to the Zero Trust policy. Endpoints cannot access applications via the SSO platform unless they are placed on the same/higher tier as the application.
			Two-factor authentication is required when logging into the virtual private network (VPN - Remote Access Service) from any internet protocol (IP) address.

Technical Safeguards – §164.312			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
			Two-factor authentication is required when launching an application from the SSO system (Idaptive).
			Multi-factor authentication is used for privileged accounts unless there is a system limitation.
			Configuration-controlled changes to infrastructure are tested, reviewed, approved, and documented.
			Configuration-controlled changes to products and services are tested, reviewed, and approved. Change management responsibilities are segregated among designated personnel.
Person or Entity Authentication	§ 164.312(d)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Formal procedures are documented that outline the process the Company's staff follows to perform the following system access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access - Restricting access based on separation of duties and least privilege
			Personal information access request policies include the requirement that personal information be provided to the requestor only after the requestor has been appropriately authenticated.
			Background checks are performed prior to an employee’s start date in compliance with local laws and regulations.

Technical Safeguards – §164.312			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
			Two-factor authentication is required when logging into the virtual private network (VPN - Remote Access Service) from any internet protocol (IP) address.
			Two-factor authentication is required when launching an application from the SSO system (Idaptive).
			Multi-factor authentication is used for privileged accounts unless there is a system limitation.
Transmission Security	§ 164.312(e)(1)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	Multi-factor authentication is used for privileged accounts unless there is a system limitation.
			Two-factor authentication is required when logging into the virtual private network (VPN - Remote Access Service) from any internet protocol (IP) address.
			Two-factor authentication is required when launching an application from the SSO system (Idaptive).
			Cryptographic mechanisms are implemented to prevent unauthorized disclosure and modification of data in transit.

Technical Safeguards – §164.312			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Integrity Controls	§ 164.312(e)(2)(i)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	Cryptographic mechanisms are implemented to prevent unauthorized disclosure and modification of data in transit.
			Customer data is logically isolated through the use of unique identifiers.
			External interfaces to the products and services and key internal interfaces are managed and monitored to prevent unauthorized use or access.
			External interfaces to the infrastructure and shared services and key internal interfaces are managed and monitored to prevent unauthorized use or access.
Encryption	§ 164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	Cryptographic mechanisms are implemented to prevent unauthorized disclosure and modification of data in transit.
			Cryptographic mechanisms are implemented or enabled to prevent unauthorized disclosure and modification of data at rest.

Organizational Requirements – §164.314			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Business Associate Contracts or Other Arrangements	§ 164.314(a)(1)	The contract or other arrangement required by § 164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.	Atlassian obtains satisfactory assurances, in accordance with § 164.314(a), that the company will appropriately safeguard the information if Atlassian creates, receives, maintains, or transmits electronic protected health information on any customer's behalf. These assurances are captured in Business Associate Agreements. Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed during the procurement process for all critical vendors.
Business Associate Contracts	§ 164.314(a)(2)(i)	The contract must provide that the business associate will-- (A) Comply with the applicable requirements of this subpart; (B) In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and (C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.	Atlassian obtains satisfactory assurances, in accordance with § 164.314(a), that the company will appropriately safeguard the information if Atlassian creates, receives, maintains, or transmits electronic protected health information on any customer's behalf. These assurances are captured in Business Associate Agreements.

Organizational Requirements – §164.314			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Business Associate Contracts	§ 164.314(a)(2)(ii)	Section 164.314(a)(2)(ii) is not relevant because Atlassian is not a covered entity.	Not applicable.
Business Associate Contracts with Subcontractors	§ 164.314(a)(2)(iii)	The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.	Atlassian obtains satisfactory assurances, in accordance with § 164.314(a), that the company will appropriately safeguard the information if Atlassian creates, receives, maintains, or transmits electronic protected health information on any customer's behalf. These assurances are captured in Business Associate Agreements.
Requirements for Group Health Plans	§ 164.314(b)	Section 164.314(b) is not relevant because Atlassian is not a group health plan.	Not applicable.

Policies and Procedures and Documentation Requirements – §164.316			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Policies and Procedures	§ 164.316(a)	Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	The HIPAA Security Compliance program is developed to ensure the security, confidentiality, and availability of UGC (and therefore, ePHI) and protect against reasonably anticipated threats or hazards to the security or integrity of ePHI. It incorporates various requirements laid out in the HIPAA Security rule, such as: - Security measures for protecting ePHI - Assessment for reasonable remediation or mitigating controls of Addressable HIPAA Security Rules - An annual HIPAA Security attestation and Gap Assessment - The regular review and retention of HIPAA Security policies and procedures - Security awareness content regarding the protection of ePHI - An annual review of the HIPAA Security Risk Analysis - The designation and role definition of a HIPAA Security Officer
Documentation	§ 164.316(b)(1)	(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	The HIPAA Security Compliance program is developed to ensure the security, confidentiality, and availability of UGC (and therefore, ePHI) and protect against reasonably anticipated threats or hazards to the security or integrity of ePHI. It incorporates various requirements laid out in the HIPAA Security rule such as: - Security measures for protecting ePHI

Policies and Procedures and Documentation Requirements – §164.316			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
			- Assessment for reasonable remediation or mitigating controls of Addressable HIPAA Security Rules - An annual HIPAA Security attestation and Gap Assessment - The regular review and retention of HIPAA Security policies and procedures - Security awareness content regarding the protection of ePHI - An annual review of the HIPAA Security Risk Analysis - The designation and role definition of a HIPAA Security Officer
Time Limit	§ 164.316(b)(2)(i)	Retain the documentation required by paragraph(b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	Formal data retention and disposal procedures are documented to guide the secure retention and disposal of Company and customer data, and requires HIPAA related documentation to be retained for at least 6 years.
			Customer data is disposed of, destroyed, or erased upon request in accordance with the retention period or upon termination of services.
			Storage media containing sensitive data and licensed software is removed and securely overwritten prior to disposal.

Policies and Procedures and Documentation Requirements – §164.316			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Availability	§ 164.316(b)(2)(ii)	Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	A security policy is shared on the Company intranet and reviewed annually.
			An incident management policy is shared on the Company intranet and reviewed annually.
			Formal procedures are documented that outline the process the Company's staff follows to perform the following system access control functions: - Adding new users - Modifying an existing user's access - Removing an existing user's access - Restricting access based on separation of duties and least privilege
			A comprehensive Code of Business Conduct and Ethics describes employee and contractor responsibilities and expected behavior regarding data and information system usage. The policy is shared and reviewed annually.
Updates	§ 164.316(b)(2)(iii)	Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment including compliance with HIPAA.
			A security policy is shared on the Company intranet and reviewed annually.
			All policies are posted and available and reviewed at least annually.

Breach Notification Rule – §164.404 - 164.414			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Notification to Individuals **Notification to the Media** **Notification to the Secretary**	§ 164.404(a) - 164.408(c)	Sections 164.404(a) through 164.408(c) are not relevant because Atlassian is not a covered entity.	Not applicable.
Notification by a Business Associate	§ 164.410(a)	(1) General rule. A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach. (2) Breaches treated as discovered. For purposes of paragraph(a)(1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).	Atlassian maintains records of customers who have signed Business Associate Agreements and reports any security incident of which it becomes aware, including breaches of unsecured ePHI, as required by the HIPAA Breach Notification Rule in 45 CFR § 164.410.

Breach Notification Rule – §164.404 - 164.414			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Timeliness of Notification	§ 164.410(b)	Except as provided in § 164.412, a business associate shall provide the notification required by paragraph(a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.	Atlassian maintains records of customers who have signed Business Associate Agreements and reports any security incident of which it becomes aware, including breaches of unsecured ePHI, as required by the HIPAA Breach Notification Rule in 45 CFR § 164.410.
Content of Notification	§ 164.410(c)	(1) The notification required by paragraph(a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. (2) A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under § 164.404(c) at the time of the notification required by paragraph(a) of this section or promptly thereafter as information becomes available.	Atlassian maintains records of customers who have signed Business Associate Agreements and reports any security incident of which it becomes aware, including breaches of unsecured ePHI, as required by the HIPAA Breach Notification Rule in 45 CFR § 164.410.

Breach Notification Rule – §164.404 - 164.414			
HIPAA Standard	**HIPAA Reference**	**Implementation Specifications**	**Applicable Control(s)**
Law Enforcement Delay	§ 164.412	If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.	Atlassian maintains records of customers who have signed Business Associate Agreements and reports any security incident of which it becomes aware, including breaches of unsecured ePHI, as required by the HIPAA Breach Notification Rule in 45 CFR § 164.410.
Administrative Requirements and Burden of Proof	§ 164.414(a)	Section 164.414(a) is not relevant because Atlassian is not a covered entity.	Not applicable.
Administrative Requirements and Burden of Proof	§ 164.414(b)	(b) Burden of proof. In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at § 164.402.	Atlassian maintains records of customers who have signed Business Associate Agreements and reports any security incident of which it becomes aware, including breaches of unsecured ePHI, as required by the HIPAA Breach Notification Rule in 45 CFR § 164.410.