Atlassian's Technical and Organisational Security Measures

Introduction

Security is an essential part of Atlassian's offerings. This page describes Atlassian's security program, certifications, policies, and physical, technical, organizational and administrative controls and measures to protect Customer Data from unauthorized access, destruction, use, modification or disclosure (the "**Security Measures**"). The Security Measures are intended to be in line with the commonly-accepted standards of similarly-situated software-as-a-service providers ("**industry standard**"), including NIST 800-53 controls.

Any capitalized terms used but not defined have the meanings set out in the Agreement or the Data Processing Addendum. Further details on Atlassian's security posture can be found in our Trust Center and Compliance Resource Center.

1. Access Control

Atlassian has implemented and will maintain a comprehensive set of formal policies, controls, and practices for the appropriate access control and protection of Customer Data, which include:

- Access management policy addressing access control standards, including the framework and the principles for user provisioning.
- Designated criticality tiers based on a Zero Trust Model architecture, including the requirements for multi-factor authentication on higher-tier services.
- User provisioning for the access to Atlassian systems, applications and infrastructure based on the relevant job role and on the least privilege principle that is enforced through the authentication processes.
- Strict role-based access controls for Atlassian staff, allowing access to Customer Data only on a need-to-know basis.
- Segregation of duties including but not limited to (i) access controls reviews, (ii) HR-application managed security groups, and (iii) workflow controls.
- A prior approval of all user accounts by Atlassian's management before granting access to data, applications, infrastructure, or network components based on the data classification level; regular review of access rights as required by relevant role.
- Use of technical controls such as virtual private network (VPN) and multi-factor authentication (MFA) where relevant based on information classification and Atlassian's Zero Trust Model architecture.
- Centrally managed mobile device management (MDM) solution, including defined lockout periods and posture checks for endpoints and mobile devices.

2. Awareness and Training

Atlassian has implemented and will maintain a comprehensive set of formal policies, controls, and practices for conducting appropriate trainings and security awareness activities, which include:

- Extensive awareness training on security, privacy, and compliance topics for all employees at induction and annually, utilizing diverse formats (online, in-person, and pre-recorded sessions, phishing simulations).
- Targeted role-specific training for employees with elevated privileges to address relevant risks and enhance their specific knowledge base.
- Maintaining of all training records in a designated learning management system.
- An automated reminder for training deadlines, with a built-in escalation process to respective managers.
- Continuous security awareness trainings (extending to contractors and partners), covering current threats and best security practices.
- Secure coding trainings by security champions embedded within engineering teams.
- Annual mandatory security trainings and events to reinforce security principles through different activities, emphasizing the collective responsibility for security.

3. Audit and Accountability

Atlassian has implemented and will maintain a comprehensive set of formal policies, controls, and practices for proper auditing and accountability purposes, which include:

- Comprehensive logging standards as part of Atlassian's policy management framework, with annual reviews and senior management approvals.
- Secure forwarding and storage of relevant system logs to a centralized log platform of the cloud infrastructure with read-only access.
- Monitoring of security audit logs to detect unusual activity, with established processes for reviewing and addressing anomalies.
- Regular updates to the logging scope of information and system events for Cloud Products and related infrastructure in order to address new features and changes.

- Utilizing time sync services from relevant cloud service providers (e.g. AWS or Microsoft Azure) for reliable timekeeping across all deployed instances.

4. Assessment, Authorisation and Monitoring

Atlassian has implemented and will maintain a comprehensive set of formal policies, controls, and practices for consistent system monitoring and security assessments, which include:

- Extensive audit and assurance policies with annual reviews and updates.
- A centralized internal policy program categorising the global policies into different domains including annual review, and senior management approval of the program.
- Audit management encompassing the planning, risk analysis, security control assessment, conclusion, remediation schedules, and review of past audit reports.
- Internal and independent external audits conducting annual evaluations of legal and contractual requirements, as well as effectiveness of controls and processes to validate compliance.
- Ongoing verification of compliance against relevant standards and regulations, e.g. ISO 27001 or SOC 2.
- Systematically addressing any nonconformities found through audit findings taking into account the root-cause analysis, severity rating, and corrective actions, all documented and tracked meticulously.
- Annual penetration testing on Products and proactive bug bounty programs for the detection and mitigation of vulnerabilities.
- Continuous vulnerability scanning, with identified vulnerabilities remediated in line with Atlassian's policy.

5. Configuration Management

Atlassian has implemented and will maintain a comprehensive set of formal policies, controls, and practices for appropriate configuration management, which include:

- Change management policies covering the risk management for all internal and external asset changes, reviewed annually.
- Standard procedures for change management applicable to encryption and cryptography for the secure handling of data (e.g. encryption keys) according to its security classification.
- A centralized internal policy program categorising the global policies into different domains including annual review, and senior management approval of the program.
- Stringent policies encompassing (i) encryption, (ii) cryptography, (iii) endpoint management, and (iv) asset tracking inline with industry standards.
- Established baselines and standards for change control that require testing documentation prior to implementation and authorized approval.
- A peer review and green build process requiring multiple reviews and successful testing for production code and infrastructure changes.
- A strict post-implementation testing and approval process for emergency changes to the code.
- Comprehensive automated system supplemented by an Intrusion Detection System (IDS), managing and protecting against unauthorized changes.
- Meticulous cataloguing and tracking of all physical and logical assets with annual reviews ensuring up-to-date asset management.

6. Contingency Planning

Atlassian has implemented and will maintain a comprehensive set of formal policies, controls, and practices for appropriate contingency planning for business continuity and disaster recovery purposes, which include:

- A skilled workforce and robust IT infrastructure, including telecommunications and technology essential for Product delivery.
- Business continuity and disaster recovery plans ("**BCDR Plans**") including defined recovery time objectives (RTOs) and recovery point objectives (RPOs).
- Business continuity plans encompassing data storage and continuity of use, reasonably designed to prevent interruption to access and utilization.
- Geographic diversity as a result of our global workforce and cloud infrastructure.
- Reinforcing business operations through resilience controls, such as daily backups, annual restoration testing, and alternative cloud infrastructure storage sites.
- A resilience framework and procedures for response and remediation of cyber events to maintain business continuity.
- Quarterly disaster recovery tests and exercises to enhance the response strategies, with post-test analyses for continuous improvement in line with the applicable BCDR Plans.
- Continuous capacity management across Products, with internal monitoring and adjustments to maintain service availability and processing capacity, for example (distributed) denial-of-service attack (DDoS) mitigation for Cloud Products and related infrastructure.

- A centralized internal policy program for annual reviews and updates of all global policies related to business continuity.
- Robust backup protocols, including (i) data encryption, (ii) redundancy across data centers, and (iii) regular testing to bolster contingency planning.

7. Identification and Authentication

Atlassian has implemented and will maintain a comprehensive set of formal policies, controls, and practices for appropriate identification and authentication purposes which include:

- Employee identification uniquely through active directory, utilising single sign-on (SSO) for application access.
- Utilising of MFA for secure access, specifically for VPN and application launch via SSO based on Atlassian's Zero Trust Model architecture.
- Password policies following the NIST 800-63B guidelines, focusing on the security aspects of password creation and management.
- Ensuring the security of stored credentials using advanced encryption methods, e.g. password and secret management systems.
- Documented approvals, regular reviews of users and accounts, and automatic syncs between the relevant identity system and HR systems to maintain the integrity and accuracy of identification data.

8. Security Incident Response

Atlassian has implemented and will maintain a comprehensive set of formal policies, controls, and practices for appropriate Security Incident response purposes, which include:

- Security Incident response plans emphasizing preparedness, containment, eradication and recovery, as well as focus on data protection and other regulatory requirements.
- Dedicated cross-functional teams handling Security Incidents, ensuring effective communication and collaboration, including well-defined processes for triaging security events.
- Regular testing of response plans with established metrics to track and improve Security Incident management effectiveness.
- Annual reviews of company-wide incident response plans and policies to reflect and share current best practices across the company.
- Post-incident review (PIR) with root cause analysis conducted for high-severity Security Incidents, focusing on systemic improvements and learning.
- Incident response procedures and plans embedded in critical business processes to minimize downtime and security risks.
- Published system availability information to aid in Security Incident handling and reporting at https://status.atlassian.com/, and https://www.loomstatus.com/, as applicable.
- The ability for Customer to report incidents, vulnerabilities, bugs, and issues, ensuring prompt attention to concerns related to system defects, availability, security, and confidentiality.
- Commitment to Customer notification of the Security Incident without undue delay under Atlassian's Data Processing Addendum, including the obligation to assist the Customer with necessary information for compliance with Applicable Data Protection Laws.

9. Maintenance

Atlassian has implemented and will maintain a comprehensive set of formal policies, controls, and practices for continued effectiveness of its Cloud Products, which include:

- Regular testing of BCDR Plans with quarterly evaluations, validated by external auditors.
- Real-time monitoring of the availability of multiple regions with performing of regular tests for infrastructure availability and reliability.
- Measures outlined in Section 4 (Assessment, Authorisation and Monitoring), Section 6 (Contingency Planning) and Section 18 (System and Communications Protection).

10. Media Protection

Atlassian has implemented and will maintain a comprehensive set of formal policies, controls, and practices to ensure the protection of media (internal and external), which include:

- Using reliable 3rd party services (e.g. Microsoft Azure or AWS) to operate the physical infrastructure for processing Customer Data as a Sub-processor.
- Sanitization and degaussing of used equipment by the 3rd party cloud service providers, including hard drives with Customer Data in line with industry standards (e.g. ISO 27001).
- Full disk encryption using industry standards (e.g. AES-256) employed for data drives on servers and databases storing Customer Data, and on endpoint devices.

- Internal bring your own device (BYOD) policy ensuring access to Customer Data is only possible via secure and compliant devices; restricting the access with technical controls (e.g. VPN) for all devices following Atlassian's Zero Trust Model architecture.
- Unattended workspaces are required to have no visible confidential data, aligning with the secure workplace guidance.

11. Physical and Environmental Protection

Atlassian has implemented and will maintain a comprehensive set of formal policies, controls, and practices for the physical and environmental protection of Customer Data, which include:

- A safe and secure working environment with controls implemented globally at Atlassian's offices.
- Employing badge readers, camera surveillance, and time-specific access restrictions for enhanced security.
- Implementing and maintaining access logs at office buildings for investigative purposes.
- Multiple compliance certifications and robust physical security measures, including biometric identity verification and on-premise security, implemented by 3rd party data center providers.
- Controlled access points and advanced surveillance systems as well as protective measures for power and telecommunication cables, alongside with environmental control systems, implemented by 3rd party data center providers.
- Positioning critical equipment in low-risk environmental areas for added safety (both by Atlassian and its 3rd party data center providers).

12. Planning

Atlassian has implemented and will maintain a comprehensive set of formal policies, controls, and practices for appropriate planning of business operations, which include:

- Active monitoring and documentation by legal and compliance teams on regulatory obligations.
- A detailed system security plan with comprehensive documentation on system boundaries and product descriptions.
- Communication to internal users and customers about significant changes to key products and services.
- Periodic reviews and updates of the security management program.

13. Program Management

Atlassian has implemented and will maintain a comprehensive set of formal policies, controls, and practices for appropriate program management, which include:

- Supporting the security management program at the executive level, encompassing all security-related policies and practices.
- Documented information security policies, including (i) defined roles, (ii) risk mitigation, and (iii) service provider security management program.
- Periodic risk assessments of systems processing Customer Data, with prompt reviews of Security Incidents for corrective action.
- Formal security controls framework aligning to standards such as SOC 2, ISO27001, and NIST 800-53.
- Processes for identifying and quantifying security risks, with mitigation plans approved by the Chief Trust Officer and regular tracking of implementation.
- Comprehensive and diverse approach to security testing to cover a wide range of potential attack vectors.
- Regular review, testing and updating of the security management program (annually, at a minimum).
- Development program for security staff with regular trainings; organizational chart that delineating roles and responsibilities.
- Setting and review of strategic operational objectives by the executive management.
- Annual review of the Enterprise Risk Management (ERM) framework, including the risk management policy, risk assessments, and fraud risk assessments, by the Head of Risk and Compliance.

14. Personnel Security

Atlassian has implemented and will maintain a comprehensive set of formal policies, controls and practices for the security of all Atlassian's employees who have access to Customer Data, which include:

- Pre-hire background checks, including criminal record inquiries, especially thorough for senior executive and accounting roles to the extent permissible under applicable local laws.
- An extensive onboarding process including confidentiality agreements, employment contracts, and acknowledgement of various policies and codes of conduct.
- Global and local employment policies, maintained and reviewed annually.
- Processes for role changes and terminations including automatic de-provisioning and checklists for employee exits, with managerial approval required for re-provisioning the access.
- Ongoing security and compliance training for employees, with targeted training for specific roles and the presence of security champions in teams.

- Hosting of annual security awareness month to reinforce security education and celebrate achievements in maintaining organizational security.
- Established disciplinary processes to manage violations of Atlassian's policies.

15. Personal Data Processing and Transparency

Atlassian has implemented and will maintain a comprehensive set of formal policies, controls, and practices for the compliance of personal data processing in line with Applicable Data Protection Laws, which include:

- A global privacy compliance program for reviewing and adapting to data protection laws including necessary safeguards and processes.
- Maintaining an internal personal data processing policy with clear definitions of personal data categories, processing purposes, and processing principles.
- Detailed standards for processing of various categories of personal data covering the topics such as processing principles, applicable legal basis, retention, destruction etc.
- An established method to create pseudonymised data sets using industry standard practices and appropriate technical and organisational measures governing the systems capable of remapping pseudonymous identifiers.
- Transparent privacy policies for its users and customers, as well as internal guidelines for employees.
- Comprehensive compliance documentation, including but not limited to (i) processing activities, (ii) privacy impact assessments, (iii) transfer impact assessments, (iv) consents, and (v) data processing agreements with customers and vendors.
- Secure development practices across all development lifecycle stages, focusing on security and data protection from the initial design phase.
- Respecting the individual's rights to access, correct, and delete their personal data in line with relevant data protection laws.

16. Risk Assessment

Atlassian has implemented and will maintain a comprehensive set of formal policies, controls, and practices for a robust Information Security Management System, which include:

- A comprehensive risk management program for identifying, assessing, and addressing various risks to support informed risk management decisions.
- A policy program aligning company-wide policies with ISO 27001 and other relevant standards to mitigate associated risks.
- Continuous security testing, including (i) penetration tests, (ii) bug bounties, and (iii) proactive threat mitigation.
- Processes and metrics for reporting vulnerability management activities.
- Thorough security evaluations, including independent external and internal audits.

17. System and Services Acquisition

Atlassian has implemented and will maintain a structured, security-centric methodology for the system development, maintenance, and change management, which include:

- An agile secure software development life cycle for the adaptability, and efficiency, as well as thorough review and documentation of system and infrastructure changes.
- Secure, standardized application deployment with automated processes for system configuration changes and deployment.
- Defined development process with peer-reviewed pull requests and mandatory automated tests prior to merging.
- Segregated responsibilities for change management among designated employees.
- Emergency change processes, including "break glass" procedures, ensuring readiness for rapid response during critical incidents.
- Robust compliance settings in Atlassian's source code and deployment systems (e.g. Bitbucket Cloud) preventing unauthorized alterations.
- Clear documentation and monitoring of all configuration changes, with automatic alerts for non-compliance or alterations in peer review enforcement.
- Strict controls over modifications to vendor software.
- Regular scanning and updates of third-party or open-source libraries as well as ongoing scanning of the code base.

18. System and Communications Protection

Atlassian has implemented and will maintain a comprehensive set of formal policies, controls, and practices for system and communication protection which include:

- Cryptographic mechanisms to safeguard sensitive information stored and transmitted over networks, including public internet, using reliable and secure encryption technologies.
- Encryption of Customer Data at rest and in transit using TLS 1.2+ with Perfect Forward Secrecy (PFS) across public networks.

- Zone restrictions and environment separation limiting connectivity between production and non-production environments.
- Continuous management of workstation assets including (i) security patch deployment, (ii) password protection, (iii) screen locks, and (iv) drive encryption through asset management software.
- Restricting access to only known and compliant devices enrolled in the MDM platform, adhering to the principles of Zero Trust Model architecture.
- Maintaining firewalls at corporate edges for both platform and non-platform hosted devices for additional layers of security.
- Network and host defense including operating system hardening, network segmentation, and data loss prevention technologies.
- Established measures to ensure Customer Data is kept logically segregated from other customers' data.

19. System and Information Integrity

Atlassian has implemented and will maintain formally established policies and practices that include the following controls and safeguards relevant for system and information integrity, in particular:

- Ongoing vulnerability scans to ensure prompt identification and remediation of vulnerabilities.
- Adherence to stringent data disposal protocols in line with applicable laws, reasonably ensuring that data from storage media is irrecoverable post-sanitization.
- Strict policies to prevent the use of production data in non-production environments, ensuring the data integrity and segregation.
- Centrally managed, read-only system logs; monitoring for Security Incidents; retention policies aligned with security best practices.
- Managing endpoint compatibility with systems and applications, enhancing network security and reliability.
- Deploying anti-malware strategies on the relevant infrastructure and Atlassian devices for robust protection against malware threats with regular updates to malware protection policies and detection tools.
- Unique identifiers and token-based access control ensure logical isolation and secure, limited access to Customer Data.

20. Supply Chain Risk Management

Atlassian has implemented and will maintain formally established policies and practices for supply chain risk management, which include:

- A formal framework for managing vendor relationships, aligning the security, availability, and confidentiality standards of suppliers throughout their lifecycle.
- A robust third party risk management (TPRM) assessment process including risk assessments, due diligence, contract management, and ongoing monitoring of all third parties
- Dedicated teams, including legal, procurement, security, and risk departments for the review of contracts, SLAs, and security measures to manage risks related to security and data confidentiality.
- Functional risk assessments for suppliers before onboarding and periodically, based on risk levels, with revisions during policy renewals or significant relationship changes.
- An inventory of all suppliers detailing ownership and risk levels associated with the services provided to Atlassian.
- Yearly review of audit reports (e.g. SOC 2) and regular reviews of IT governance policies and security assessments of supply chain to ensure controls are both, appropriate and effectively compliant.
- Measures to secure third-party endpoints, focusing on compliance monitoring and selective restrictions based on the mobile & bring your own device policy.