JiBrok Security Questionnaire

Note: This Questionnaire was derived from the CAIQ Lite (https://cloudsecurityalliance.org/star/caiq-lite/)

Section Heading	Control Heading	Original ID	Question Text	Answer	Notes/Comment
General	General	Gen-01.1	Name of Third-Party / Vendor	JiBrok	
		Gen-02.1	Responder Name	-	
		Gen-03.1	Responder Job Title	-	
		Gen-04.1	How long has the company been in business?	Since 2018	
		Gen-05.1	Any material legal claims or judgments against the company?	No	
		Gen-06.1	Please describe the service(s) provided?	JiBrok is an Atlassian Marketplace Partner that provides apps for Jira. They are a Jira app developer and offer a range of tools and features such as message banners, HTML display settings, conditions, dynamic messages, JavaScript, time calculation, etc.	JiBrok specializes in developing applications for Jira, focusing on enhancing functionality and user experience. Their products include tools for tracking time in various statuses, setting timers and stopwatches, and creating calculated custom fields. They offer solutions for both Jira Data Center and Jira Cloud, providing features like dynamic messages, user delegation, and field panels for Jira Service Management. JiBrok aims to streamline workflow management and improve productivity for Jira users.
Application & Interface Security	Application Security	AIS-01.2	Do you use an automated source code analysis tool to detect security defects in code prior to production?	Yes	Github, Bitbucket, Amazon CodeGuru, SonarQube, Snyk
		AIS-01.5	(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	Yes	All deployments to production occur only after a personal code review. This includes checking automatic changes from Snyk and similar tools.
	Customer Access Requirements	AIS-02.1	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and information systems?	Yes	
	Data Integrity	AIS-03.1	Does your data management policies and procedures require audits to verify data input and output integrity routines?	Yes	
Audit Assurance & Compliance	Independent Audits	AAC-02.1	Do you allow tenants to view your SOC 2/ISO 27001 or similar third-party audit or certification reports?	Yes	Via JiBrok Trust Center https://jibrok.com/security/
		AAC-02.2	Do you conduct network penetration tests of your cloud service infrastructure at least annually?	Yes	
		AAC-02.3	Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?	Yes	
	Information System Regulatory Mapping	AAC-03.1	Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	Yes	This is implemented via the Information Security Policy
Business Continuity Management & Operational Resilience	Business Continuity Testing	BCR-02.1	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Yes	JiBrok conducts an Annual Business Continuity / Disaster Recovery Tabletop Exercise
	Policy	BCR-10.1	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	Yes	This is implemented via the Business Continuity Plan and Disaster Recovery Plan
	Retention Policy	BCR-11.1	Do you have technical capabilities to enforce tenant data retention policies?	Yes	
		BCR-11.3	Have you implemented backup or recovery mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	Yes	This is implemented via the Backup Policy
		BCR-11.7	Do you test your backup or redundancy mechanisms at least annually?	Yes	JiBrok conducts an Annual Business Continuity / Disaster Recovery Tabletop
Change Control & Configuration	Unauthorized Software Installations	CCC-04.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	Yes	This is implemented via the Acceptable Use Policy and Information Security Policy
Data Security & Information Lifecycle Management	E-commerce Transactions	DSI-03.1	Do you provide standardized (e.g. ISO/IEC) non-proprietary encryption algorithms (3DES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?	Yes	This is implemented through Heroku
		DSI-03.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)?	Yes	This is implemented via the Encryption Policy
	Non Production Data	DSI-05.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	Yes	This is implemented via the Encryption Policy and Software Development Lifecycle Policy
	Secure Disposal	DSI-07.1	Do you support the secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data?	Yes	This is implemented via the Data Retention Policy
		DSI-07.2	Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	Yes	This is implemented via the Data Retention Policy
Datacenter Security	Asset Management	DCS-01.2	Do you maintain a complete inventory of all of your critical assets located at all sites/ or geographical locations and their assigned ownership?	Yes	JiBrok reviews and updates its Asset Inventory at least quarterly
	Controlled Access Points	DCS-02.1	Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) implemented for all areas housing sensitive data and information systems?	Not Applicable	JiBrok does not have a physical location.
	User Access	DCS-09.1	Do you restrict physical access to information assets and functions by users and support personnel?	Not Applicable	JiBrok does not have a physical location.

Encryption & Key Management	**Key Generation**	EKM-02.1	Do you have a capability to allow creation of unique encryption keys per tenant?	Yes	
	Encryption	EKM-03.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	Yes	This is implemented via the Encryption Policy. Encryption is implemented
Governance and Risk Management	**Baseline Requirements**	GRM-01.1	Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?	Yes	Policies are made available to employees through our internal GRC program.
	Policy	GRM-06.1	Are your information security policies and procedures made available to all impacted personnel and business partners, authorized by accountable business role/function and supported by the information security management program as per industry best practices (e.g. ISO 27001, SOC 2)?	Yes	Policies are made available to employees through our internal GRC program.
	Policy Enforcement	GRM-07.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	Yes	This is implemented via the Human Resources Security Policy
	Policy Reviews	GRM-09.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	Yes	https://jibrok.com/blog/
		GRM-09.2	Do you perform, at minimum, annual reviews to your privacy and security policies?	Yes	JiBrok conducts an Annual Policy review via Drata
Human Resources	**Asset Returns**	HRS-01.1	Upon termination of contract or business relationship, are employees and business partners adequately informed of their obligations for returning organizationally-owned assets?	Not Applicable	JiBrok does not have any employees or contractors but this is covered in the Human Resources Security Policy
	Background Screening	HRS-02.1	Pursuant to local laws, regulations, ethics, and contractual constraints, are all employment candidates, contractors, and involved third parties subject to background verification?	Not Applicable	JiBrok does not have any employees or contractors but this is covered in the Human Resources Security Policy
	Employment Agreements	HRS-03.1	Do your employment agreements incorporate provisions and/or terms in adherence to established information governance and security policies?	Not Applicable	JiBrok does not have any employees or contractors but this is covered in the Human Resources Security Policy
	Employment Termination	HRS-04.1	Are documented policies, procedures, and guidelines in place to govern change in employment and/or termination?	Yes	JiBrok does not have any employees or contractors but this is covered in the Human Resources Security Policy
	Training / Awareness	HRS-09.5	Are personnel trained and provided with awareness programs at least once a year?	Yes	JiBrok conducts. Annual Security & Awareness Training via Drata.
Identity & Access Management	**Audit Tools Access**	IAM-01.1	Do you restrict, log, and monitor access to your information security management systems (e.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)?	Yes	This is implemented via the System Access Control Policy
		IAM-01.2	Do you monitor and log privileged access (e.g., administrator level) to information security management systems?	Yes	This is implemented via the System Access Control Policy
	User Access Policy	IAM-02.1	Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?	Yes	This is implemented via the System Access Control Policy
	Policies and Procedures	IAM-04.1	Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?	Yes	This is implemented via the System Access Control Policy
	Source Code Access Restriction	IAM-06.1	Are controls in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only?	Yes	This is implemented via the System Access Control Policy
		IAM-06.2	Are controls in place to prevent unauthorized access to tenant application, program, or object source code, and assure it is restricted to authorized personnel only?	Yes	This is implemented via the System Access Control Policy
	User Access Restriction / Authorization	IAM-08.1	Do you document how you grant, approve and enforce access restrictions to tenant/ customer credentials following the rules of least privilege?	Yes	JiBrok conducts Quarterly User Access Reviews of all Critical and High Risk Level applications
	User Access Reviews	IAM-10.1	Do you require a periodical authorization and validation (e.g. at least annually) of the entitlements for all system users and administrators (exclusive of users maintained by your tenants), based on the rule of least privilege, by business leadership or other accountable business role or function?	Yes	JiBrok conducts Quarterly User Access Reviews of all Critical and High Risk Level applications
	User Access Revocation	IAM-11.1	Is timely deprovisioning, revocation, or modification of user access to the organizations systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties?	Yes	JiBrok conducts Quarterly User Access Reviews of all Critical and High Risk Level applications
Infrastructure & Virtualization Security	**Audit Logging / Intrusion Detection**	IVS-01.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis, and response to incidents?	No	
		IVS-01.2	Is physical and logical user access to audit logs restricted to authorized personnel?	Yes	JiBrok conducts Quarterly User Access Reviews of all Critical and High Risk
		IVS-01.5	Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?	Yes	Audit logs are reviewed on a regular basis for security events through the
	Clock Synchronization	IVS-03.1	Do you use a synchronized time-service protocol (e.g., NTP) to ensure all systems have a common time reference?	Yes	Yes, Heroku utilizes a synchronized time-service protocol such as NTP (Network Time Protocol) to ensure that all systems maintain a common
	OS Hardening and Base Controls	IVS-07.1	Are operating systems hardened to provide only the necessary ports, protocols, and services to meet business needs using technical controls (e.g., antivirus, file integrity monitoring, and logging) as part of their baseline build standard or template?	Yes	In Heroku, operating systems are hardened to provide only the necessary ports, protocols, and services to meet business needs. This is achieved through the implementation of technical controls such as antivirus
	Production / Non-Production Environments	IVS-08.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	Yes	
		IVS-08.3	Do you logically and physically segregate production and non-production environments?	Yes	Test and production environments are different applications in Heroku that
	Segmentation	IVS-09.1	Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?	Yes	Firewalls are configured by Heroku
	VMM Security - Hypervisor Hardening	IVS-11.1	Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls and TLS-encapsulated communications to the administrative consoles)?	Yes	
	Wireless Security	IVS-12.1	Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?	Yes	
		IVS-12.2	Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings)?	Yes	

		IVS-12.3	Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?	Yes	
Interoperability & Portability	**APIs**	IPY-01.1	Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?	Not Applicable	JiBrok's cloud applications currently don't have a public API. For applications in the Data Center, the API is published via postman.
Mobile Security	**Approved Applications**	MOS-03.1	Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores can be loaded onto a mobile device?	Not Applicable	JiBrok does not have mobile devices
Security Incident Management, E-Discovery, & Cloud Forensics	**Incident Management**	SEF-02.1	Do you have a documented security incident response plan?	Yes	
		SEF-02.4	Have you tested your security incident response plans in the last year?	Yes	
	Incident Reporting	SEF-03.1	Are workforce personnel and external business relationships adequately informed of their responsibility, and, if required, consent and/or contractually required to report all information security events in a timely manner?	Yes	
		SEF-03.2	Do you have predefined communication channels for workforce personnel and external business partners to report incidents in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations?	Yes	
	Incident Response Legal Preparation	SEF-04.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?	Yes	
Supply Chain Management, Transparency, and Accountability	**Incident Reporting**	STA-02.1	Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?	Yes	Yes, this is also an atlassian requirement. They have instructions on what to do and how to notify the client(by email).
	Network / Infrastructure Services	STA-03.1	Do you collect capacity and use data for all relevant components of your cloud service offering?	Yes	
	Third Party Agreements	STA-05.4	Do third-party agreements include provision for the security and protection of information and assets?	Yes	This is implemented via the Vendor Managemenmt Policy and Annual Vendor Security Reviews of compliance reports
		STA-05.5	Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	Yes	Daily backups occur in Heroku.
	Supply Chain Metrics	STA-07.4	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	No	
	Third Party Audits	STA-09.1	Do you mandate annual information security reviews and audits of your third party providers to ensure that all agreed upon security requirements are met?	Yes	This is implemented via the Vendor Managemenmt Policy and Annual Vendor Security Reviews of compliance reports
Threat and Vulnerability Management	**Antivirus / Malicious Software**	TVM-01.1	Do you have anti-malware programs that support or connect to your cloud service offerings installed on all of your IT infrastructure network and systems components?	Yes	Supported through Heroku
	Vulnerability / Patch Management	TVM-02.5	Do you have a capability to patch vulnerabilities across all of your computing devices, applications, and systems?	Yes	JiBrok uses Snyk for vulnerability scanning and remediation
	Mobile Code	TVM-03.1	Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?	Not Applicable	JiBrok does not have mobile devices