Security and Risk Assessment Overview

Due to the volume of requests received, Idera, Inc.and its subsidiaries (collectively “Idera”) are unable to complete individual security due diligence, ethical compliance, and risk assessment questionnaires. Below is an overview of Idera’s Governance, Risk, and Compliance (GRC) posture and technical and organizational security measures.

Additional information beyond what is available on Idera’s corporate legal webpage requires that the requestor has either a signed customer agreement or a Non-Disclosure Agreement (NDA) in place. Please contact your Idera Account Manager for access to the following: copies of available security certifications, policy table of contents, Certificates of Insurance (COI’s), SIG Lite and CAIQ questionnaires.

Summary of Content

Idera, Inc. Security Program

Idera, Inc. and all its subsidiaries (collectively “Idera”) maintains a written security program that complies with applicable global industry recognized information security frameworks (for example, NIST, OWASP, and AICPA’s Trust Services Criteria), includes administrative, technical and physical safeguards reasonably designed to protect the confidentiality, integrity and availability of Customer Data, and is appropriate to the nature, size and complexity of Idera’s business operations.

Idera’s corporate policies, standards, and operating procedures are reviewed, updated (as needed), and approved on an annual basis or more frequently as needs arise to maintain their continuing relevance and accuracy. All Idera personnel are required to review and acknowledge security policies during on-boarding and annually thereafter.

Idera’s Chief Security Officer and compliance group develop, maintain, review and approve all Company policies. These policies undergo further review by Idera’s counsel and independent third-party SOC 2 auditors.

All Idera personnel are required to complete compliance and security awareness training at the time of hire and on an annual basis thereafter.

Encryption and Key Management

Idera uses industry-standard encryption techniques to encrypt Customer Data at rest and in transit when applicable. All connections are authenticated and encrypted using industry standard encryption technology.

Incident Response and Notification

Idera has an incident response plan, including a breach notification process, to assess, escalate, and respond to identified physical and cyber security incidents that impact the organization, customers, or result in data loss. Discovered intrusions and vulnerabilities are resolved in accordance with established procedures. The incident response plan is reviewed and updated annually and more frequently as needed.

If there is a breach impacting Customer Data, Idera will notify any affected parties without undue delay upon discovery of the breach, reasonably cooperate with respect to investigations, and take appropriate corrective action to mitigate any risks or damages to protect Customer Data from further compromise. Idera will take any other actions that may be required by applicable law.

Risk Management

Idera has a security risk assessment and management process to identify and remediate potential threats to Idera and its customers. Risk ratings are assigned to all identified risks, and remediation

is managed by the compliance team in conjunction with stakeholders from applicable departments. Executive management is kept apprised of the risk posture of the organization.

Access Control

Idera assigns application and data rights based on security groups and roles, which are created based on the principle of least privilege. Security access requests are reviewed and approved by the applicable stakeholder prior to provisioning access.

Informational assets are classified in accordance with Idera's data classification guideline.

User Access Management

All access to Idera systems and networks are disabled promptly upon notification of termination or departure.

Idera reviews administrator access to confidential and restricted systems, including corporate and cloud networks, on a regular basis. Administrator access to the cloud production environment and to select corporate systems that provide broad privileged access are reviewed on a quarterly basis.

Idera uses separate administrative accounts to perform privileged functions, and accounts are restricted to authorized personnel.

Password Management and Authentication Controls

Authentication mechanisms require users to identify and authenticate to the corporate network with their unique user ID and password. Idera requires minimum password parameters for the corporate network via a directory service system. Remote access to the corporate network is secured through a virtual private network (VPN).

Threat and Vulnerability Management

Idera's Vulnerability Management program monitors for vulnerabilities on an on-going basis using a combination of internal and external vulnerability scans using industry-recognized vulnerability scanning tools. Identified vulnerabilities are evaluated, documented and remediated to address the associated risk(s).

External penetration tests are conducted annually by an independent third party. Significant findings from these tests are evaluated, documented and remediated.

Logging and Monitoring

Idera continuously monitors application, infrastructure, network, data storage space and system performance using anti-malware, anti-virus, and threat detection tools. Security events trigger alerts which are promptly reviewed by authorized personnel. Access to logs is restricted to

authorized personnel and reviewed both automatically and manually. Logs contain details on the date, time, source, and type of events.

Change Management

Idera has change management policies and procedures for requesting, testing and approving application, infrastructure and product related changes. All changes receive a risk score based on risk and impact criteria. Low risk changes generate automated change tickets and have various levels of approval based on risk score. High risk changes require manual change tickets to be created and are reviewed by approvers based on change type. Planned changes to the corporate or cloud production environments are reviewed regularly. Change documentation and approvals are maintained in a ticketing system.

Product development changes undergo various levels of review and testing based on change type, including security and code reviews, regression, and user acceptance testing prior to approval for deployment. Following the successful completion of testing, changes are reviewed and approved by appropriate managers prior to implementation to production. Idera, Inc. uses dedicated environments separate from production for development and testing activities. Access to move code into production is limited and restricted to authorized personnel.

Secure Development

Idera has a software development life cycle (SDLC) process, consistent with the corporate security policies, that governs the acquisition, development, implementation, configuration, maintenance, modification and management of Idera's infrastructure and software components. Prior to the final release of a new Idera system version to the production cloud environment, code is pushed through lower tier environments for testing and certification. Idera follows secure coding guidelines based on leading industry standards.

These guidelines are updated as needed and provided to all applicable personnel. Idera, Inc. utilizes a code versioning control system to maintain the integrity and security of the application source code.

Software and Asset Inventory

Idera maintains an inventory of all software components (including, but not limited to, open-source software) used in Idera products, and inventory of all media and equipment where Customer Data is stored.

Idera, Inc. reviews the legal terms and requirements of all software components and updates, as applicable, and includes references to source materials or any such relevant terms in its inventory.

Data Management

This section is applicable solely for the Idera entities that offer Software as a Service. Idera Customer Data will only be hosted in data centers that have attained SOC 2 Type 2 attestations

or have ISO 27001 certifications (or equivalent or successor attestations or certifications). Idera backs up all Customer Data in accordance with Idera's standard operating procedure. Customer Data is only kept for the duration of the contract or as long as there is a business purpose or legal obligation.

Customers can request copies of their data or to have their data removed at any time by contacting compliance@idera.com.

Workstation Security

Idera implements and maintains security mechanisms on personnel workstations, including firewalls, anti-virus, and full disk encryption. All onsite personnel are required to follow clean desk guidelines and lock or log off of devices when away from workstations.

Network Security

Idera uses network perimeter defense solutions, including IDS and firewalls, to monitor, detect and prevent malicious network activity. Security personnel monitor items detected and take appropriate action.

Firewall rule changes (that meet the criteria for the corporate change management criteria) follow the change management process and require approval by the appropriate stakeholders. Idera's corporate and cloud networks are logically segmented by virtual local area networks (VLANs) and firewalls monitor traffic to restrict access to authorized users, systems and services.

Third Party Security

Idera assesses and manages the risks associated with existing and new third-party vendors and employs a risk-based scoring model for each third party. Idera requires all third parties to enter into contractual commitments that contain security, availability, processing integrity and confidentiality requirements and operational responsibilities as necessary.

Idera evaluates the physical security controls and assurance reports for data centers on an annual basis, assesses the impact of any issues identified and tracks any remediation efforts.

Physical Security

Idera's operations are primarily remote based. Idera restricts access to its facilities, equipment, and devices to employees with authorized access on a need-to-know basis. Any access to physical locations is reviewed and determined by job responsibility, and access is removed as part of the Idera separation or internal job transfer process when access is no longer required.

All access to Idera facilities is managed by a logged badging system and CTV surveillance.

Oversight and Audit

Internal audits are aligned to Idera's information security program and compliance requirements. Idera conducts internal control assessments to validate that controls are operating effectively. Issues identified from assessments are documented, tracked and remediated.

Internal controls related to security, availability, processing integrity and confidentiality are audited by an external independent auditor at least annually and in accordance with applicable regulatory and industry standards.

Business Continuity and Disaster Recovery Plan

Idera maintains a Business Continuity Plan and a Disaster Recovery Plan to manage significant disruptions to operations and infrastructure. These plans are reviewed, updated, and approved by the Chief Security Officer on an annual basis.

Idera conducts periodic business continuity exercises to evaluate tools, processes and subject matter expertise in response to specific incidents. Results of these exercises are documented and issues identified are tracked to remediation.

Human Resources Security

Idera has standard procedures in place to guide the hiring process. Background verification is required for Idera personnel in accordance with relevant laws and regulations. Idera requires personnel to sign a confidentiality agreement as a condition of employment.

All personnel are also required to review and acknowledge Idera's Information Security policy, which includes acknowledging responsibility for reporting security incidents involving Customer Data. Idera maintains a disciplinary process to take action against personnel that do not comply with company policies, including Idera security policies.

HIPAA

Any Idera personnel with access to protected health information (PHI) are required to complete new hire and ongoing annual HIPAA training. All Idera personnel are required to adhere to HIPAA rules and regulations.

GDPR/ Data Privacy Legislation

Idera continuously reviews and adheres to all global data privacy legislation with assistance from in-house counsel and a third-party data privacy vendor. All Idera personnel receive data privacy training at the time of hire as well as on an annual basis thereafter. Idera vendors, subprocessors, and contractors with access to Customer Data are required to sign a Data Processing Agreement (DPA).

Customer DPA's are available for all Idera SaaS products on the applicable legal webpage for that brand under "Legal Terms & Customer Agreements." Idera's Universal Customer-Facing DPA includes the European Union 2021 Standard Contractual Clauses (SCC's) and the United Kingdom ("UK") International Data Transfer Agreement and the UK Transfer Addendum and has the following Exhibits:

- Universal Customer-Facing Data Processing Agreement
- Data Processing Terms (each SaaS product has its own Data Processing Terms, which includes a list of subprocessors and data hosting locations on the applicable entity's legal web page under "Policies & Procedures.")
- Jurisdiction Specific Terms

Ethical and Export Compliance

Idera adheres to Export and Trade regulations and Idera's Export Compliance Policy is available on the legal webpage. All Idera policies regarding ethical compliance matters (i.e. Anti-Bribery, Anti-Slavery, Code of Conduct, etc.) are available on each entity's legal webpage under "Policies & Procedures."

Security Certifications

The following Idera entities have completed a SOC 2 audit:

- Xblend (Xray and Xporter)
- BitTitan (moving to ISO 27001:2013 certification in 2023*)
- Gurock
- Kiuwan
- PreEmptive
- Assembla
- Qubole
- Perspectium
- Filestack

The following Idera products will have a NIST 800-171 self-assessment report available in 2023:

- SQL Diagnostic Manager
- SQL Compliance Manager
- Ranorex Studio
- Designwise
- Travis CI
- ER/Studio Business Architect
- ER/Studio Data Architect
- ER/Studio Software Architect
- Team Server

- Yellowfin
- Wherescape Red
- Wherescape 3D
- DBArtisan

Active customers may request copies of an audit report by contacting their Idera Account Manager. Prospective customers will be required to sign an NDA with the applicable brand's sales team (contact information is available on the product's website).

*BitTitan is a Microsoft Supplier and since Microsoft recently announced that only ISO certifications will be accepted from Suppliers, BitTitan is changing from the SOC 2 audit process to ISO certification.

Idera Corporate Policies

The following are Idera's governing documents for all entities:

- Anti-Slavery and Human Trafficking
- Anti-Bribery
- Application Security
- Business Continuity and Disaster Recovery
- Change Management and Control
- Data Governance
- Data Retention and Destruction
- Data Storage
- Encryption Management
- Export Compliance
- General Information Security
- Idera and its subsidiaries Code of Conduct
- Incident Management
- Information Security Management System
- Internal Audit
- Network Security
- Privacy Statement
- Privileged Access
- Risk Management
- Security Statement
- Software Development Lifecycle
- System Access Management
- System Hardening
- Third-Party Vendor Diligence
- User Access Control
- Vendor Code of Conduct
- Vulnerability and Patch Management

Idera does not disclose full policies to external parties, however these policies have been reviewed in their entirety by an independent third-party auditor as part of the SOC 2 audit process.

Active customers may request copies of the Table of Contents for each policy from their Idera Account Manager. Prospective customers will be required to sign an NDA with the applicable brand's sales team (contact information is available on the product's website).