HireVue Information Security Overview

Document Classification:	**HireVue - Public**
Date:	**06/03/2021**

Service Provider Name/Location	HireVue, Inc. 10876 S. River Front Pkwy, #500 South Jordan, UT 84095	**Service Provider Contact Information (Name, Phone, Email)**	Information Security Team 801-316-2910 privacy@hirevue.com

HireVue provides on demand (one-way) and live (two-way) video interviews for job applicants, interview coordination, chatbot, and game based assessments. Managers create interviews, invite candidates, review interviews, and share with other evaluators. Interviews may be scored, rated, and commented on. Confidential information includes user and candidate names, email addresses, video/audio interviews, and any interview ratings or scores.

HireVue services are hosted through Amazon Web Services (AWS) using Amazon's state-of-the-art data centers with locations around the world. HireVue's digital interview management platform has been engineered to scale as needed while maintaining the high level of security standards that are required by global financial, consumer, and healthcare organizations to protect confidential information.

Penetration Testing

Annually, the HireVue system is put through a manual penetration test performed by a third party security firm. The exhaustive testing includes a review of source code and covers the OWASP and SANS methodologies. All vulnerabilities are triaged and significant issues are remediated in accordance with HireVue's vulnerability management policy. A copy of the most recent test can be made available to interested third parties upon request,under NDA.

Security Controls

Information about HireVue's policy, procedures, and practices in the following security control areas is commonly requested. This document provides a general overview of these areas. More details and answers to specific security related questions are available upon request. Additional details on specific controls can also be found in HireVue's SOC 2 Type 2 audit report, which is available under NDA and covers HireVue's Video Interviewing, Assessments, and Coordinate products in scope.

Security Control	Concern	HireVue Solution
1. Governance – Policies and Procedures	Security policies and procedures are in place that govern secure service delivery and protection of customer data.	HireVue has established a comprehensive data security policy and Information Security Management System in accordance with ISO/IEC 27001:2013.
2. Compliance	Evidence of assessments that are periodically performed to ensure compliance with policies, procedures, regulatory requirements, etc.	HireVue has undergone SOC 2 auditing, and our most recent SOC 2 Type 2 report is available to interested third parties under NDA. This report considered the Trust Services Principles and Criteria for Security, Availability, and Confidentiality

		HireVue received initial ISO 27001 certification on January 26, 2018. HireVue's current certification was issued by Cadence Assurance and can be provided upon request. The HireVue platform is hosted exclusively using Amazon Web Services, which is itself ISO 27001 compliant and performs annual SSAE 16 audits. A copy of the Amazon SOC 2 report is available upon request to Amazon and under their NDA.
3. Physical Security	Physical security perimeter safeguards in place (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols).	HireVue offices are generally paperless with all management, control, monitoring, and administration of the platform being handled remotely using credentialed access over encrypted connections from various locations. The entire HireVue application and data is hosted through Amazon AWS, which adheres to common practices for physical security.
4. User Access	Restricted access to information assets for internal users, support personnel and customers.	All access to customer information is controlled via unique accounts and multi-factor authentication. There is no physical access allowed by customers or HireVue to the Amazon physical facilities. Access to customer-specific data is controlled logically through the use of permissions on data objects with permissions associated with roles and groups. All access is on a need-to-know basis.
5. Network Security – Perimeter Network	Safeguards implemented in the perimeter network to protect internal assets from unauthorized access.	Perimeter network security is provided by Amazon in their Virtual Private Cloud (VPC). All system access is logged internally in a centralized logging system. Two-factor authentication is required for all access to Amazon-based HireVue production servers.
6. Network Security – Internal Network	Safeguards implemented in the internal network to protect the internal assets in case the perimeter network has been breached.	Internal assets are defined as application software, system generated data (administration, analytics, logs), and customer data. Production application software and services are only available through a controlled process. Admin/analytics/logs information is available to internal users with proper roles and credentials and according to organizational policy and controls. Customer data, while contained in a single database, is logically isolated with access restricted by account-level controls and only with appropriate credentials. All access to servers and services is protected using a front-side firewall controlled via security

		groups. Access to internal services is further protected using a VPN server configured to require multi-factor authentication. A network diagram is available on request.
7. Network Security – Wireless / Guest Network	Wireless and guest access provisioned with security safeguards in place.	HireVue offices provide wireless access to the Internet for employees and guests, and both require WPA2 passwords. However, there is no internal network with locally hosted servers or site-to-site VPN that could put customer data at risk. All customer data is hosted in AWS.
8. Operations Security – Capacity / Resource Planning	Availability, quality, and adequate capacity and resources are planned, prepared, and measured to deliver the required system performance.	The HireVue service has been designed to provide capacity “on demand” with the ability to add incremental capacity at any point in the system in a matter of minutes when load reaches predetermined thresholds. All servers, services, and connections are continuously monitored for health and load. In the event that a trigger point is reached, new capacity is added well before any critical level is reached.
9. Operations Security – Change Management	How changes are controlled and applied to production environments.	HireVue’s change control procedures are established and part of standard operating procedure. All planned changes are categorized by potential impact to the service, business, and customers. A formalized roll-back plan is in place in the event that any change negatively impacts service delivery supported by adequate monitoring and performance measurement tools.
10. Operations Security – Anti-Virus Checks	How the environment is protected against virus infections and malware infiltration.	Workstations used in support of the environment implement anti-virus software to actively monitor for the presence of malicious files or software. All files uploaded by users to our servers are scanned for viruses before being processed or stored.
11. Operations Security – Logging & Monitoring	How logging, monitoring, reporting, and alerting is implemented to verify effectiveness of security controls and access policies.	All user access logs are retained and reviewed using automation, continually and manually, once each week. All server/service logs are aggregated to a central log server where they are analyzed and retained for a period of no less than 3 years. Alerts are generated on anomalies and reports are maintained for manual review.
12. Operations Security – Incident Management / Reporting Incidents	Incident Management process and how security incidents are reported to customers.	HireVue has implemented a formal incident response plan, under the management of a designated Security Incident Response Team (SIRT). Upon activation of the plan, the SIRT will evaluate, contain, and eradicate the source of the incident. Should an incident result in a

		material breach that impacts clients, those clients will be notified without undue delay or inline with the notification terms defined in service agreements.
13. Information Security – Access Control	Access control mechanisms and the associated processes in place that ensure proper authentication and authorization of users.	The HireVue application has various standard roles for customers to use for rights management. Documentation of roles and permissions is available upon request. Each user role has specific role privileges to objects and only objects within a customer account are accessible. Internal HireVue users have Operations Support roles with the ability to “proxy” into specific customer accounts. This “proxy” activity is logged. All Ops Support personnel are only given access to customer information on a need-to-know basis. HireVue users who are terminated have access revoked generally within one hour.
14. Information Security – Application Security	Processes and procedures in place to ensure the web application is built using secure coding best practices and is not vulnerable to known web application attacks.	HireVue develops software according to an Agile methodology and is continually releasing with approximately two-week sprints. The architecture is N-tier. The HireVue development approach is iterative and utilizes continuous integration so all changes seen by multiple developers are immediately regression tested. All failures are immediately addressed by the team. The software is designed to have high levels of automated testing to minimize potential of regression. The development team performs code reviews prior to integration. The build process is metric driven and the process is designed to keep software in a running state at all times. High levels of automated UI testing are implemented that operate across multiple platforms and browsers. All production data in the development and QA environments is anonymized to protect customer data. Customer data is segregated logically with an account element associated with each data object. Permissions limit visibility and access only to objects within an account according to roles, groups, and account memberships. Penetration tests are performed regularly by HireVue customers, and at least annually by a third party firm on behalf of HireVue. Vulnerability scans are performed by HireVue on a biweekly basis.

15. Information Security – User Credentials Management	Controls for user credentials management are implemented and enforced.	SAML 2.0 integration is currently offered, which allows account password controls to be under the control of the customer. For those who prefer to not implement SAML 2.0 integration, the following password controls are in place. a. Passwords can be reset by users through the email address associated with the account. b. Revocation for account users (customers) is delegated to customer account admins. c. All user IDs must be unique and also be a valid email. d. Password policies such as password expiration, minimum password length, password character set requirements, password reuse constraints, user lock-out requirements, and session time-outs for inactivity can be customized by the customer upon request. e. User logs for session initiation are maintained.
16. Data Governance – Segregation	Levels of data segregation.	Data is logically separated by account element. All production data is anonymized in any non-production environment.
17. Data Governance – Encryption	How sensitive corporate and customer data is protected using encryption.	HireVue data consists of candidate information, user information, video interview, and interview ratings/comments. This information is always encrypted in transit. All video is encrypted in transit using TLS, or DTLS-SRTP. All backups, resumes, and digital interviews are encrypted at rest using AES 256.
18. Data Governance – Backup and Retention	Data backup and data retention policies and procedures.	Backups are continuous with at least two copies onsite at the Amazon hosting center. A third backup is available from a second location. Amazon does not backup data outside of Amazon hosting facilities.
19. Resiliency – BCP / DRP	Business Continuity and Disaster Recovery Plans.	HireVue has developed Business Continuity and Disaster Recovery Plans that include documented procedures for business, IT, and development functions in the event of any number of scenarios. Plans include contingent locations, trigger events, key personnel responsibilities and backups, customer communication procedures, and recovery time objectives.
20. Human Resources Security	Policies, procedures, and processes are in place to ensure secure hiring and termination of employees.	All employees are required to sign confidentiality agreements and go through a 360º reference and background check

		before accessing any customer data. In the event of termination, all company assets are retrieved and data access is removed without undue delay.. Employees also complete privacy and security training upon hire, and annually, thereafter.