HireTeamMate, Inc.

(dba hireEZ)

System and Organization Controls

(SOC 3) Report

For the Period from

March 1, 2021 through February 28, 2022

Frank, Rimerman + Co. LLP

System and Organization Controls (SOC 3)
Report on the hireEZ® Platform Relevant to
Security, Availability, and Confidentiality

For the Period from March 1, 2021 through February 28, 2022

Table of Contents

Section I – Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls Relevant to the Applicable Trust Services Criteria

HireTeamMate, Inc. (dba hireEZ)
Mountain View, California

Certified Public Accountants

Scope

We have examined HireTeamMate, Inc. (dba hireEZ) (the Company) management assertion in Section II of this report titled "Assertion Provided by HireTeamMate, Inc.'s Management" (assertion) that the controls within the Company's hireEZ® Platform (the Platform) were effective throughout the period from March 1, 2021 to February 28, 2022, to provide reasonable assurance the Company's 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* (American Institute of Certified Public Accountants (AICPA), Trust Services Criteria).

Attachment A within this report, titled "Description of the HireTeamMate, Inc.'s Platform" indicates complementary user-entity controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. 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.

Service Organization's Responsibilities

The Company is responsible for identifying the Platform and describing the boundaries of the Platform, its service commitments and system requirements and for designing, implementing, and operating effective controls within the Platform to provide reasonable assurance the Company's service commitments and system requirements were achieved. The Company is responsible for providing the assertion about the effectiveness of controls within the Platform. When preparing its assertion, the Company is responsible for selecting the trust services categories, identifying, the applicable trust service criteria on which the assertion is based, and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the Platform.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the Platform were effective throughout the period to provide reasonable assurance the service organization's service commitments and system requirements were achieved throughout the period from March 1, 2021 to February 28, 2022, based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination involves performing procedures to obtain evidence about the assertion and includes:

- Obtaining an understanding of the Platform and the Company's service commitments and system requirements.

- Assessing the risks the controls were not effective to achieve the Company's service commitments and system requirements based on the applicable trust services criteria.

- Performing procedures to obtain evidence about whether controls within the Platform were effective to achieve the Company's service commitments and system requirements based on the applicable trust services criteria.

- Testing the operating effectiveness of controls to provide reasonable assurance the Company achieved its service commitments and system requirements based on the applicable trust services criteria.

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

Our examination was not conducted for the purpose of evaluating the Company's cybersecurity risk management program. Accordingly, we do not express an opinion on any other form of assurance on its cybersecurity risk management program.

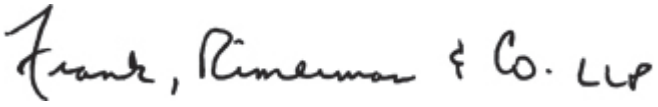
Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk the controls may become inadequate because of changes in conditions or the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within the Company's Platform were effective throughout the period from March 1, 2021 to February 28, 2022, to provide reasonable assurance the Company's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



San Jose, California
May 17, 2022

Section II – Assertion Provided by HireTeamMate, Inc.'s Management

We are responsible for designing, implementing, operating, and maintaining effective controls within HireTeamMate, Inc. (dba hireEZ)'s (the Company) hireEZ® Platform (the Platform) throughout the period from March 1, 2021 to February 28, 2022, to provide reasonable assurance the Company's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the Platform is presented in Attachment A within this report, titled "Description of the HireTeamMate, Inc.'s Platform" and identifies the aspects of the Platform covered by our assertion.

In designing the controls over the Platform we determined certain trust services criteria can only be met if complementary user-entity controls are suitably designed and operating effectively for the period from March 1, 2021 to February 28, 2022.

We have performed an evaluation of the effectiveness of the controls within the Platform throughout the period from March 1, 2021 to February 28, 2022, to provide reasonable assurance the Company's 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* (AICPA, Trust Services Criteria). The Company's objectives for the Platform in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B within this report, titled "The Principal Service Commitments and System Requirements".

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance its service commitments and system requirements are achieved.

We assert to the best of our knowledge and belief, the controls within the Platform were effective throughout the period from March 1, 2021 to February 28, 2022, to provide reasonable assurance the Company's service commitments and system requirements were achieved based on the applicable trust services criteria, if user-entity controls assumed in the design of the Company's controls throughout the period from March 1, 2021 to February 28, 2022.

HireTeamMate, Inc.

/s/ Xinwen Zhang
Chief Technology Officer/Co-Founder
May 17, 2022

Attachment A – Description of the HireTeamMate, Inc.'s Platform

A. Company Overview

Founded in 2015, HireTeamMate, Inc. (dba hireEZ) (hireEZ or the Company) is headquartered in Mountain View, California. hireEZ is a Software as a Service (SaaS) company that makes outbound recruiting easy, by enabling customers, also referred to as talent acquisition teams, to target prospective candidates quickly with the use of artificial intelligence (AI) technology. The Platform searches and recommends candidates from multiple platforms and helps customers build hiring pipelines based on the defined job requirements and engage the candidates. The Platform also provides talent analytics based on the search criteria and helps users make effective recruiting strategies.

B. Services Provided

The report covers the Platform offerings described below. The major features of the Platform are:

- EZ Sourcing - Identifies the strongest candidates across multiple platforms on the web and ensures results are the best match according to the job description. In addition, AI Sourcing SM has the ability to track potential candidates through different hiring stages allowing hiring managers and recruiters to be more effective in their hiring efforts.

- EZ Pipeline - Produces a customized hiring pipeline to fit a customer's needs in one centralized location to manage across systems and applications.

- EZ Engagements - Integrates with industry-standard email systems to contact and automatically follow up with candidates or contact multiple candidates at once.

- EZ Integrations - Enables recruiting workflows through integrations with the customer's applicant tracking system (ATS) and/or customer relationship management (CRM) system.

- EZ Insights - Prioritize limited resources and keep pace with the changing needs of an organization and see how to compare with others in an industry. Understand where to strategically invest the customer's recruiting workforce.

- EZ Collaboration - Ensure the smooth flow of a teams' hiring processes with a user-friendly portal that is rich with flexible, clear, and easy-to-toggle feature settings and configurations, improved metrics, and performance tracking.

C. Scope

The scope of this report is limited to the Platform throughout the period from March 1, 2021 to February 28, 2022 based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC2® Report* (AICPA Description Criteria) and the controls to achieve hireEZ's

service commitments and system requirements relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in Trust Services Principles and Criteria (TSP) 100, *2017 Trust Services Criteria (TSC) for Security, Availability, Confidentiality, Processing Integrity, and Privacy* (AICPA, Trust Services Criteria).

Subsequent Events

Management is not aware of any relevant events that occurred subsequent to the end of the reporting period through the date of the independent service auditor's report that would have a significant effect on management's assertion.

Response to Okta Security Incident

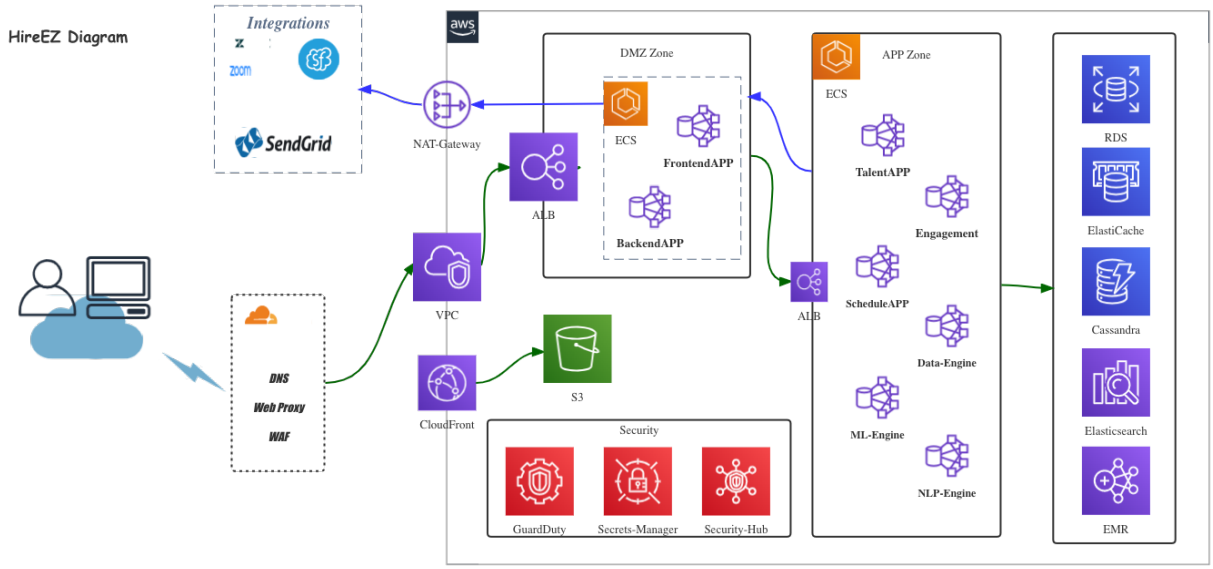
During the period, the Company utilized identity and access management services provided by Okta, Inc. (Okta). In January 2022, Okta was subject to a security incident whereby approximately 2.5% of its customers were potentially impacted as a result of their data being viewed or acted upon. In March 2022, Okta publicly disclosed the security incident that occurred in January 2022. As a result of the security incident disclosure by Okta, the Company performed a thorough investigation and determined there was no compromise of the Company's customer data. Following the disclosure by Okta of the security incident, management responded by conducting a thorough investigation into the impact of the incident to the Platform itself. Company management determined the Platform had not been impacted by the security incident. In March 2022, Okta confirmed the Company's instance had not been compromised as a result of the security incident.

D. Components of the Platform Used to Provide Services

The boundaries of the Platform are the specific aspects of the Company's infrastructure, software, people, processes and procedures, and data necessary to provide its services. Any infrastructure, software, people, and data indirectly supporting the services provided to customers are not included within the boundaries of the Platform. The components directly supporting the services provided to customers are described below.

Infrastructure

hireEZ infrastructure uses a virtual private cloud (VPC) hosted by Amazon Web Services, Inc. (AWS) to launch the core hireEZ web application, underlying databases, machine learning engines, and monitoring applications to protect the Company, customer, and talent data, and users accessing this data.



Software

The Platform is a web-based multi-tenant, cloud-based SaaS offering. hireEZ leverages industry-standard third-party software tools to support the Platform. There are three key categories of software tools used: 1) system configuration and provisioning software, 2) source code management software, and 3) monitoring software.

People

Company personnel provide support and services in each of the core functional areas supporting the Platform, including Engineering, Development Operations (DevOps), and Security engineers, Customer Success, Human Resources (HR), and Legal. Each functional area is overseen by Senior Management.

Processes and Procedures

Management has established and implemented policies and procedures to ensure periodic assessments and evaluations are performed that consider elements of security, availability, and confidentiality as they apply to the AICPA TSC.

The Company has developed formal security and confidentiality policies and operational procedures that are reviewed annually by the Chief Technology Officer. All hireEZ personnel must adhere to hireEZ policies and procedures that address services to be delivered. The policies include control activities that are designed and implemented for each major functional area.

Data

The Company collects, aggregates, stores, and provides access to real-time talent information. This data is stored in the Platform database and used to support customer needs to acquire new candidates and to provide customers with historical visibility and activities of customer usage of the Platform.

The data collected and stored by hireEZ is defined and classified within the Company's policies. Customer usage and activity data are classified as customer confidential data. Talent information is not considered customer confidential data as it is aggregated from public records or purchased by hireEZ from data vendors. The Company has deployed secure methods and protocols for the transmission of data over public networks. Encryption is enabled on databases housing sensitive customer data.

Novel Coronavirus (COVID-19)

The outbreak of COVID-19 has adversely impacted global commercial activity. The Company has been impacted by governmental restrictions that have been placed on all entities, which have not been identified as "essential businesses", preventing it from conducting operations from its offices. These restrictions require Company personnel to perform their job responsibilities while working from home. Management believes the design and operating effectiveness of the control environment, and systems supporting the Platform will allow the Company to continue to meet its customer commitments and achieve its service commitments and system requirements relevant to the applicable trust services criteria during the period of uncertainty caused by COVID-19.

E. Subservice Organization

The Company uses AWS, a subservice organization for the Platform infrastructure hosting services, including data center hosting, physical security, environmental safeguards, and redundant infrastructure. The Company monitors the quality of AWS's performance and reviews the subservice organization's SOC 2 Type 2 reports covering activities related to the security, availability, and confidentiality TSC.

F. Relevant Aspects of the Control Environment

The Company's internal control environment is governed and managed by the Company's Board of Directors (the Board), management, and other personnel working on the achievement of objectives related to the effectiveness and efficiency of the Company operations while being in compliance with applicable laws and regulations.

Control Environment

The Company's commitment to an effective system of internal controls is led by Senior Management and overseen by the Board. The Board, composed of both founders and an investor operating independently from the Company's management, manages, provides guidance, and ensures business and Company's objectives are met. Senior Management

meets with the Board periodically to communicate the current state of the business, including security and compliance-related updates.

The control environment at the Company is the foundation for all areas of internal controls. Senior management recognizes its responsibility for directing and controlling operations, managing risks, and establishing, communicating, and monitoring control policies and procedures. Organizational charts are in place to communicate the defined key areas of authority, responsibility, and lines of reporting to personnel supporting system design, development, implementation, security, operation, maintenance, and monitoring. The current management structure has adequate segregation of responsibilities across the Senior Management team to ensure no overriding influence exists within the current reporting structure.

Senior Management emphasizes the implementation and adherence to controls and ethical behavior throughout the Company. The overarching business principles and standards of conduct contained within the Employee Handbook define the core values of the integrity expected of personnel. The handbook discusses the use of the Company's electronic resources and explains the importance of adherence to the Company's standards of conduct. The handbook also includes an enforcement section detailing disciplinary action for non-compliance with the Company's policies.

These principles are supported by a set of Company-wide commitments, standards, and requirements defining how the Company is governed. The Company has also developed a set of security-related policies as well as operational procedures outlining Company requirements to protect and secure assets and data and to hold individuals accountable for their internal control responsibilities.

The Company has established policies and practices related to employee recruiting, hiring, onboarding, training, and performance evaluation. Evaluation of potential candidates emphasizes business experience, past accomplishments, technical competence, and cultural fit within the defined values at the Company. Once the offer letter has been signed, the HR team initiates a third-party background check, which includes a Social Security number trace, and local, state, and federal background investigations for criminal history. To ensure new hires are aware of their obligation to protect Company information and customer data, the HR team requires new hires to sign confidentiality agreements noting their agreement to protect Company confidential information. Formal performance reviews are conducted annually to aid in the continuous improvement process for the employee and the control environment.

Communication and Information

The Company has established an overarching Security, Confidentiality, and Data Protection Policy that notes the roles, responsibilities, and overall rules to achieving the Company's information security goals. Company personnel participate in the security awareness training ensuring their awareness of Company policies.

The Company informs customers of the Company commitments to the security of the Platform and confidentiality of the data stored within the Platform within a Service Order Form and Master Services Agreement (MSA). The Company also communicates the Terms of Service

(TOS) and Data Processing Agreement (DPA) to customers through its public-facing website. The Company's website also contains the Platform description and tutorials describing the features and functionality of the Platform. Changes made to the Platform are posted within the Company's web application informing authenticated users of updates.

Risk Assessment

The Company understands the necessary balance between risk and control, and the intent of risk management is to reduce risk to an acceptable level. The Company attempts to reduce business risk through an annual information security risk assessment when management identifies critical assets, the threats facing those assets, and the likelihood and impact of the security of the assets that could be compromised. Senior Management reviews applicable laws and regulations, and the impact of new laws and regulations on the Company, as well as risks related to significant changes in production systems, key personnel, or operational environment. Risks are reviewed, assigned an owner, and remediated within a timeframe based on criticality and Platform impact. Additionally, the results of internal and external audits, customer findings, and other compliance activities are collated and form the basis for the risk assessment process.

The Company management performs a risk review of third-party vendors and business associates and reviews contracts to ensure the protection of customer data and the Company's systems. The Company reviews the subservice organization's SOC report or equivalent annually to evaluate the subservice organization's controls and their alignment with hireEZ's security, availability, and confidentiality commitments.

Monitoring

The Engineering team monitors the Platform for security and availability using a combination of internal and external tools. Cloud security monitoring tools are used to identify anomalies and issues, as well as to detect intrusions and vulnerabilities. Additional monitoring tools are configured to alert on-call DevOps personnel to triage and remediate performance issues, as necessary. An independent third-party vendor performs an annual application penetration test against the Platform. Management reviews identified vulnerabilities, and high-risk issues are assessed for mitigation and resolution.

Senior Management engages a third-party consultant to conduct an internal review of the Company's internal controls. When changes to internal controls occur, they are evaluated, agreed upon by the control owners, documented, and communicated in the Company's internal workspace. Results from the internal control review and from control owners are communicated to Senior Management. These scheduled activities are captured and recorded on the compliance calendar to remind personnel of their responsibility for maintaining their internal controls tasks.

G. Complementary User-Entity Controls (CUECs)

Security is a shared responsibility between the Company and its customers. The Platform was designed with the assumption certain controls would be implemented by the user entities (customers). Certain requirements can be met only if the complementary user entity controls are suitably designed and operating effectively, along with related controls at the Company. Platform users should consider whether the following controls have been placed in operation at their organizations:

User entities are responsible for:
Complying with the Terms of Service and contractual agreements to prevent unauthorized access to or use of the Platform, and notify the Company immediately of any such unauthorized access.
Complying with all applicable laws, rules, and regulations.
Cooperating with the Company in establishing a password or other procedures for verifying that only designated customer end users have access to any administrative functions of the Platform.
Maintaining the security of the customer end users account and passwords, including administrative users passwords.
Performing periodic reviews of user access to the customer account.
Not knowingly providing or allowing access to the Platform to any person who is not an authorized user of the customer.
Not sharing with any third party any account or password without the prior written consent of the Company.
Sending data through to the Company using only a secure connection.
Reviewing changes made by administrators within their environment.

H. Significant Changes in Controls to the Platform

The Company has not made any significant changes to its control environment since the previous examination period.

Attachment B – The Principal Service Commitments and System Requirements

The Company makes service commitments to its customers and has established system requirements as part of the Platform. Some of these commitments are principal to the performance of the Platform and relate to the AICPA TSC relevant to security, availability, and confidentiality (applicable trust services criteria). The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the Platform to provide reasonable assurance its service commitments and system requirements are achieved based on the applicable trust services criteria.

Service commitments to customers are documented and communicated in a Service Order Form, MSA, the TOS, and the DPA. The TOS can be found on the Company's website at https://app.hireez.com/policies/termsofservice#menu-term-of-use. Service commitments include but are not limited to, security, availability, and confidentiality.

Availability

The Company has made commitments related to percentage uptime and connectivity for the Platform, as well as commitments related to service credits for instances of downtime.

The Company is architected in a manner to maintain the availability of its services through defined programs, processes, and procedures. Contingency plans and incident response procedures are maintained to reflect emerging continuity risks and lessons learned. Plans are tested, updated through the course of business, reviewed annually, and approved by Senior Management.

Security and Confidentiality

The Company has made commitments related to securing and maintaining the confidentiality of customer data and complying with relevant laws and regulations. These commitments are addressed through measures including confidentiality terms, data encryption, authentication mechanisms, and other relevant security controls.

The Company has also implemented technical controls designed to prevent unauthorized access to or disclosure of content. Internally, confidentiality requirements are communicated to employees through training and policies. Company personnel are required to attend security awareness training, which includes information, policies, and procedures related to protecting customers' data. In addition, the Company monitors the third parties used through annual periodic reviews by evaluating performance against contractual obligations, including confidentiality commitments.

The Company has established operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in the Company system policies and procedures, system design documentation, and contracts with customers. Information security policies define a Company-wide approach to how systems and data are protected. These policies include how the Platform is designed and developed, how the system is operated, how the internal business systems and networks supporting the Platform are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of various services provided by the Platform.