Notice at Collection and Privacy Policy for Employees in Multiple States, including California, Nevada, and Virginia

ZPE Systems Inc.

Effective Date: November 16, 2023

Respecting the privacy of employees, interns, independent contractors, job applicants, board members, etc. of ZPE Systems Inc. is an essential feature of the privacy program. ZPE Systems Inc. and its subsidiaries and affiliated companies (the "**Company**") take your privacy seriously. We want you to know how we collect, use, and disclose your personal information, and your rights with regards to such information.

For employees, independent contractors, job applicants, interns, board members, etc., please take notice that the Company collects certain information about you. For ease of reference, individuals who reside in and/or perform work for the Company in states such as California, Nevada, or Virginia, regardless of their employment status with the Company, will all be referred to here as "applicants and employees". For example, while independent contractors are not employees of the Company, for ease of reference in this policy, they are referred to as "applicants and employees".

This Notice at Collection and Privacy Notice for Employees Who Reside in Multiple States ("Multi-State Employee Privacy Notice" or "Multi-State Notice") is adopted to comply with the current state laws regarding privacy in California, Nevada, and Virginia, including California Consumer Privacy Act (CCPA) 2018, Cal. Civil Code Section 1798.100 et. seq., as amended by the California Privacy Rights Act (CPRA), the Virginia Consumer Data Protection Act ("VCDPA"), and the Privacy and Security of Personal Information Chapter of the Nevada Revised Statutes Section 603A ("603A"), and related regulations, and as may be further amended from time to time. This Multi-State Employee Privacy Notice applies solely to the Company's employees, contractors or job applicants who reside and/or perform work in California, Virginia, or Nevada. Any terms defined in the CCPA, as amended by the CPRA, in the VCDPA, and/or in 603A, have the same meaning when used in this Notice.

This Multi-State Employee Privacy Notice applies to the Company's offline and online data collection practices, including when you submit personal data for purposes of applying for and/or becoming a valued employee at the Company, and in the course of your employment with us, pursuant to applicable state law. This Multi-State Employee Privacy Notice describes the types of personal information that the Company may collect from you as an employee and the purposes for collecting such information. Information on your rights with respect to such personal information is also described in this Notice and who to contact to exercise those rights.

1. Your Rights.

The applicable state laws, including the California Consumer Privacy Act **("CCPA"**) and California Privacy Rights Act **("CPRA")** provides applicable state applicants and employees with certain rights:

- Knowledge of information collected.
- Deletion of information collected.
- Opt-out of information collected.
- Opt-in of information collected.
- Correction of information collected.
- Go to court.
- Limit use of information collected.
- Not to be discriminated against or retaliated against for exercising rights under the law.

2. <u>Where We Get Your Information From</u>. The Company collects information about you from the following sources: 1) you; 2) prior employers, references, recruiters, job-related social media platforms; 3) third-party sources of demographic information; 4) third-party companies, such as background check companies, drug testing facilities; and 5) claim administrators and investigators. Depending on the Company's interactions with you, we may or may not collect all of the information identified about you.

3. <u>The Personal and Sensitive Personal Information That We Are Collecting</u>. We may collect the following information:

- Identifiers, such as name, government-issued identifier (*e.g.*, Social Security number), and unique identifiers (*e.g.*, employee ID);
- Personal information, such as real name, signature, Social Security Number (SSN), physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, passport number, federal identification authorizing work in the United States, access and/or passcodes, insurance policy number, education, employment, employment history, bank account number, other financial information, medical information, or health insurance information.
- Characteristics of protected classifications under California, Nevada, Virginia, or federal law, such as age, marital status, gender, sex, race, color, disability, citizenship, primary language, immigration status, military/veteran status, disability, request for leave, and medical conditions.
- Commercial information, such as transaction information and purchase history (*e.g.*, in connection with travel or other reimbursements);
- Internet or network activity information, such as browsing history and interactions with the Company's online systems and websites and any personal information that you

provide while accessing the Company's computer systems, such as personal credit card information and passwords.

- Geolocation data, such as device location from usage of the Company's devices.
- Biometric information related to access to the Company's secured access points.
- Audio, electronic, visual, and similar information.
- Professional or employment-related information, such as work history and prior employer.
- Non-public education information.
- Personal communications, such as the contents of mail, email, or text messages on accounts or services not owned, or subscribed to, by Company only for purposes of legitimate Company investigations and, to the extent required by law, with your authorization; and
- Inferences drawn from any of the Personal and Sensitive Personal Information listed above to create a profile or summary about, for example, an individual's preferences and characteristics.

4. <u>How Your Personal and Sensitive Personal Information is Used</u>. We may use Personal and Sensitive Personal Information:

- To operate, manage, and maintain the Company's business;
- For hiring, retention, and employment purposes;
- To otherwise accomplish the Company's business purposes and objectives, including, for example:
    - Emergency services;
    - Conducting research, analytics, and data analysis;
    - Maintaining the Company's facilities and infrastructure;
    - Quality and safety assurance measures;
    - Conducting risk and security controls and monitoring;
    - Protecting confidential and trade secret information;
    - Detecting and preventing fraud;
    - Performing identity verification;

- Performing accounting, audit, and other internal functions, such as internal investigations;
- Complying with the law, legal process, and internal policies;
  - Maintaining records;
  - Claims processing;
  - Responding to legal requests for information and subpoenas; and
  - Exercising and defending legal claims.

- Any other purposes authorized by the applicable state agency or law, including the California Privacy Protection Agency, California, Virginia, Nevada or Federal law.

We may or may not have used Personal and Sensitive Personal Information about you for each of the above purposes.

5. <u>Sharing of Personal Information</u>. The Company generally maintains information related to its applicants and employees as confidential; however, from time to time, we may have a legitimate business need to disclose personnel information for one of the purposes noted above, to one or more of the categories of recipients listed below. In that event, we disclose your personal information and/or sensitive personal information only to the minimum extent necessary to achieve the purpose of the disclosure and only if the disclosure is permitted by the CPRA and other applicable laws. Categories of recipients includes:

- **Service providers and contractors**: We may disclose your personal information to service providers and contractors to assist us in meeting the Company's business needs and contractual and legal obligations;
- **Affiliated companies**;
- **Clients and customers**: This may include, for example, disclosing a sales representative's contact information with clients and customers;
- **Business partners**: For example, we might disclose your business contact information to a co-developer of a new product or service with which you will be working;
- **Government or administrative agencies**: These may include, for example: Internal Revenue Service to pay taxes, the Employment Development Department as required for state payroll taxes and to respond to unemployment or state disability insurance claims, OSHA/CalOSHA as required to report work-related death or serious injury or illness, Department of Fair Employment and Housing as required to respond to employment charges; and California Department of Industrial Relations as required to resolve workers' compensation claims.

- **Public**: We may disclose your personal information to the public as part of a press release, for example, to announce promotions or awards. If you do not want your personal information in press releases, please contact the HR Department at hr@zpesystems.com. We do not disclose sensitive personal information to the public.

- **Required Disclosures**: We may be required to disclose personal information (a) in a court proceeding, (b) in response to a court order, subpoena, civil discovery request, other legal process, or (c) as otherwise required by law.

- **Legal Compliance and Protections**: We may disclose personal information when we believe disclosure is necessary to comply with the law or to protect the rights, property, or safety of a Company, the Company's users, or others.

6. Selling of Personal Information. The Company **DOES NOT** sell your personal information.

7. Data Retention. The Company retains the information it receives about you for a period of 3 years, unless a shorter or longer period is required by California or Federal law.

We will store your personal data, in a form that permits us to identify you, for no longer than is necessary for the purpose for which the personal data is processed. We store your personal data as necessary to comply with the Company's legal obligations, resolve disputes, and enforce the Company's agreements and rights, or if it is not technically and reasonably feasible to remove it. Otherwise, we will seek to delete your personal data within a reasonable timeframe upon request.

8. Rights Under the CCPA and CPRA. Under California law, as an employee, you are afforded several rights, as discussed further below, about the personal information collected about you. However, there are several exceptions that may apply. These exceptions to the right to request to access, correct, amend, and/or delete your personal information may include the Company's right to maintain personal information of employees for business purposes and solely internal uses reasonably aligned with the expectations of the employee, as well as to comply with any legal obligations, including maintaining proper employee records, or maintaining privilege or confidentiality of certain records, in compliance with applicable U.S. and California labor laws and legal rights.

Right to Know About Personal Information Collected or Disclosed

Personal Information Collected

In the past 12 months, we have collected the following categories of personal information about California employees: personal identifiers, financial information, biometric information, sensitive personal information, health, and internet/network/IT information.

Information Sold or Shared

Right to opt-out of sale or share of personal information:

Taking into account possible exceptions, you have the right to opt-out of the sale or share of your personal information. In general, the Company does not sell or share personal information. More specifically, we have not sold or shared personal information about California employees in the past 12 months.

We have disclosed the following categories of personal information about California employees for a business or commercial purpose in the preceding 12 months:

- IP address, device ID, browser type, domain names, access times and dates, pages viewed, one or more cookies that may uniquely identify your browser, referring website addresses, what applications are run on your company issued device, files downloaded, opened, and created using company managed equipment, geolocation of laptops and mobile devices which contain company data, and any personal information entered into any company controlled system, including company email.

- Name, job title, mailing address, right to work for I-9 verification, phone number, date of birth, gender, names and relationships of dependents, emergency contact information, credit check, background check, resume with professional, employment and educational background, language proficiency, beneficiary designations, garnishment notices from tax agencies, proof of identification, health information, diversity information and EEO data collection.

Requests to Know

You have the right to request that we disclose personal information we collect about you.

To make a request for any of the information set forth above (a "Request to Know"), please submit a verifiable employee request pursuant to the instructions below. You may only make a Request to Know twice within a 12-month period. We will acknowledge your Request to Know within 10 days and will attempt to respond substantively within 45-90 days.

The Request to Know must provide sufficient information to allow us to verify that you are the person about whom the personal information was collected or disclosed and must contain sufficient detail to allow us to properly understand, evaluate and respond to your request. If we cannot verify your identity, we will not be able to respond to your request.

You can make a Request to Know the personal information we have about you by contacting us at **hr@zpesystems.com**

Once we receive your Request to Know, we will begin the process to verify that you are the person that is the subject of the request (the "Verification Process"). The Verification

Process consists of matching identifying information provided by you with the information we have about you in the Company's records.

Right to Known Sensitive Personal Information Collected

We collect and use your Sensitive Personal Information, which includes personal identification numbers, including social security, driver's license, passport, or state ID card numbers; banking information; diversity and EEO data collection including race and ethnicity, sexual orientation, military and disability status. We do not collect or process sensitive personal information for the purpose of inferring characteristics or for any purpose other than those set forth in CPRA Regulations, Article 3, Section 7027(m).

Right to Request Deletion of Personal Information

You have the right to request the deletion of your personal information collected or maintained by the Company ("Request to Delete"), subject to certain exceptions permitted by law.

To make a Request to Delete, please submit a verifiable employee request pursuant to the instructions below. We will acknowledge your Request to Delete within 10 days and will attempt to respond substantively within 45-90 days.

The Request to Delete must provide sufficient information to allow us to verify that you are the person about whom the personal information was collected, sold or disclosed and must contain sufficient detail to allow us to properly understand, evaluate and respond to your request. If we cannot verify your identity, we will not be able to respond to your request. Additionally, as permitted by law, if the information requested to be deleted is necessary for us to maintain, we will not be able to comply with your request. We will notify you if this is the case.

You can make a Request to Delete by contacting us at hr@zpesystems.com

Once we receive your initial request to delete and your separate confirmation to delete, we will need to verify that you are the person that is the subject of the request (the "Verification Process"). The Verification Process consists of matching identifying information provided by you with the information we have about you in the Company's records.

We will retain correspondence, documents and information related to any Request to Know, Request to Delete, or Request to Opt-Out for 24 months, as required by law.

Right to Correct

You have the right to request that we rectify inaccurate information about you.

Requests to Correct

To make a Request to Correct, please submit a verifiable employee request pursuant to the instructions below. We will acknowledge your Request to Correct within 10 business days and we will attempt to respond substantively within 45-90 days.

You can make a Request to Correct by contacting us at hr@zpesystems.com

Once we receive your request to correct, we will need to verify that you are the person that is the subject of the request through the Verification Process.

We will review all information provided by you to us, to determine whether the information is inaccurate. We reserve the right to delete the information instead of correcting if such deletion does not impact you or you consent to the deletion.

We will inform you of the Company's decision to deny or grant your request.

We will retain correspondence, documents and information related to any Request to Correct for 24 months as required by law.

Right to opt-in

California residents have the right to request that personal information collected from minors under the age of 16 opt-in to the collection and use of their personal information.

Right to Non-Discrimination for Exercising Consumer Privacy Rights

You have the right not to receive discriminatory treatment for exercising your privacy rights conferred by the CCPA, including by exercising the rights specified herein.

Retention of Personal Information

The Company retains your Personal Information as long as necessary to facilitate the employment (contractor or prospective employee) relationship, or for other essential purposes such as complying with the Company's legal obligations, maintaining business and financial records, resolving disputes, maintaining security, detecting and preventing fraud and abuse, or for any other necessary business purpose.

Authorized Agent Information

You may designate an authorized agent to make a request on your behalf under the CCPA. When your authorized agent makes a request related to your personal information, we will require the agent to provide the above written permission. We may also require that you verify your own identity directly with us at the time such a request is made.

During the course of your employment, you will be required to provide certain information including your name and email address to certain third parties for access to necessary software platforms and services. These third-party companies have their own privacy policies, and though they must be compliant with the Company's privacy

policies, you should review their privacy notices to understand how they utilize information. Any request regarding how they use your information must be addressed to that company.

Other Virginia Privacy Rights

Right to Appeal

As a Virginia resident, you have the right to appeal our refusal to take action on, or respond to, a verified request. Upon receipt of our denial or refusal to take action on, or to respond to, a verified request, a Virginia resident has 60 days to submit a request to appeal our decision by contacting us at hr@zpesystems.com. Within 60 days of the receipt of your appeal request, we will inform you in writing of any action taken or not taken in response. We will also include a written explanation of the reasons for our decision. If your appeal is denied, you have the right to contact the Virginia Attorney General at (804) 786-2071.

Right to Opt-Out of Certain Profiling

You have the right to opt out of our use of profiling when used to make decisions that produce a legal or similarly significant effect concerning you or your interactions with us. Currently, ZPE Systems Inc. does not engage in such profiling.

Nevada Privacy Notice

If you are a Nevada resident, under Privacy and Security of Personal Information Chapter of the Nevada Revised Statutes Section 603A ("603A"), we are required to provide notice that ZPE Systems Inc. does not sell personally identifiable information and does not have plans to start.

9. Changes to this Privacy Policy. If we change this Privacy Policy, we will post those changes on this page and update the Privacy Policy Effective Date above. If we materially change this Privacy Policy in a way that affects how we use or disclose your personal information, we will provide prominent notice of such changes and the effective date of the changes before making them.

10. Governing Law

This Notice along with the Company's privacy practices will be subject exclusively to the laws of the State of California, United States of America. We make no representation that this Notice and its practices comply with the laws of other jurisdictions.

11. Consent

Please review this Employee Privacy Notice periodically. You should read this entire Notice before submitting information, including personal information, to us in any form. Whenever you submit personal information to us, you consent to the collection, use, disclosure, transfer, and storage of that information in accordance with this Notice.

All personal information may be used for the purposes stated in this Notice. We may make full use of all information that is de-identified, aggregated, or otherwise not in personally identifiable form.

12. For Inquiries and/or to Submit Requests for Information, Deletion or Correction.
Please contact either: (1) hr@zpesystems.com or (2) 844-497-3797 for inquiries about the Company's policy, or to submit your requests for information, deletion, or correction.

If applicable, we may need to verify the identity of the individual submitting the request.