NETFORCE GLOBAL EU US AND SWISS PRIVACY SHIELD PRIVACY POLICY

NetForce Global, LLC ("NetForce Global") complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. NetForce Global has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/

NetForce Global also complies, where applicable, with U.S. law. In the event of a conflict between this Privacy Shield Privacy Statement and other applicable laws, NetForce Global will comply with its obligations under the applicable law. NetForce Global's Privacy Shield Privacy Statement is organized around the following principles:

1. NOTICE

At NetForce Global, we notify individuals about the purposes for which we collect and use information about them, choices they have regarding certain uses and disclosures of their personal data, and how to contact us with inquiries or complaints. We provide this notice either directly, such as through this privacy statement, or through our customers.

NetForce Global collects personal data for the purpose of providing a variety of information products and services to employers and other NetForce Global customers. For example, NetForce Global may collect identification information and information such as information about an individual's employment history, educational qualifications, professional qualifications, credit history, driving history, or criminal history for the purpose of providing this information to our customers.

2. CHOICE

In many cases, the reports that we prepare are prepared with the express consent of the individual. For example, the subject of a consumer report issued for employment purposes must provide express authorization ("opt-in"), typically through the employer or prospective employer, before NetForce may furnish the report. In other cases, NetForce offers individuals the opportunity to choose (opt-out) whether their personal data is (i) to be disclosed to a third party (other than our service providers performing tasks on NetForce's behalf pursuant to a contract or a customer on whose behalf we are processing it) or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals.

For sensitive information (defined at the end of this section), NetForce obtains (directly or through a third party, such as our customer) affirmative express consent (opt-in) from individuals, with certain exceptions permitted by the Privacy Shield program, if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice.

We are committed to providing individuals with clear, conspicuous, and readily available mechanisms to exercise choice. Therefore, in addition to any other mechanisms that may be provided in particular cases, individuals may opt-out by contacting NetForce using the points of contact in the "Contact Us" section

below.

Sensitive information for purposes of this policy means personal data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, information specifying the sex life of the individual or information designated by the transferring organization as sensitive. In the case of information transferred pursuant to the Swiss Privacy Shield, sensitive information also includes information on social security measures or administrative or criminal proceedings and sanctions, which are treated outside pending proceedings.

3. ACCOUNTABILITY FOR ONWARD TRANSFER

NetForce Global discloses personal data that it collects to the customer that requested it. NetForce Global may disclose personal data to its service providers. NetForce Global also may be required to disclose personal data in response to lawful requests by public authorities, including disclosures to meet national security or law enforcement requirements. NetForce Global's disclosure of personal data to third parties is governed by the Notice and Choice Principles described above.

When transferring personal data to our customers or other third-party controllers (i.e., entities that will control how personal data is processed), we comply with the Notice and Choice Principles as described above. Consistent with Privacy Shield timing requirements for onward transfer compliance, NetForce Global will enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual, that the recipient will provide the same level of protection as the Principles, and the recipient will notify the NetForce Global if it makes a determination that it can no longer meet this obligation. The contract shall provide that when such a determination is made, the third party controller ceases processing or takes other reasonable and appropriate steps to remediate.

As noted above, NetForce Global also may transfer personal data to service providers acting on its behalf. In such cases, consistent with Privacy Shield timing requirements for onward transfer compliance, NetForce Global will:

i. transfer such data only for limited and specified purposes;
ii. ascertain that the service provider is obligated to provide at least the same level of privacy protection as is required by the Privacy Shield Principles;
iii. take reasonable and appropriate steps to ensure that the service provider effectively processes the personal data transferred in a manner consistent with NetForce Global's obligations under the Principles;
iv. require the service provider to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles;
v. upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and
vi. provide a summary or a representative copy of the relevant privacy provisions of its contract with that service provider to the Department of Commerce upon request.

4. SECURITY

NetForce Global takes reasonable and appropriate measures to protect personal data from loss,

misuse, and unauthorized access, disclosure, alternation, and destruction, taking into account the risks involved in the processing and nature of the personal data.

5. DATA INTEGRITY AND PURPOSE LIMITATION

NetForce Global limits the personal data it collects to information that is relevant for the purposes of processing. NetForce Global does not process personal data in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, NetForce Global takes reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current.

NetForce Global takes reasonable and appropriate measures to retain personal data only for as long as NetForce Global has a legitimate legal or business need to do so, such as customer service, compliance with legal or contractual retention obligations, retention for audit purposes, security and fraud prevention, preservation of legal rights or other reasonable purposes consistent with the purpose of the collection of the information. NetForce Global will adhere to the Principles for as long as it retains personal data transferred in reliance upon the Privacy Shield.

6. ACCESS

It is NetForce Global's policy to provide individuals with access to personal data about them that NetForce Global holds about them and provides them with a means to request the correction, amendment, or deletion of that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

NetForce Global requires that an individual provide reasonable verification of their identity before we provide access to personal data. To access your NetForce Global file and obtain any of the remedies discussed in this section please contact NetForce Global using the point of contact in the "Contact Us" section below.

7. RECOURSE, ENFORCEMENT AND LIABILITY

NetForce Global internally monitors and assesses our compliance with our Privacy Shield Privacy statement and our Privacy Shield obligations. Under the Privacy Shield Principles, NetForce Global may be liable in the event that a service provider to whom NetForce Global transfers personal data such personal data in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage. An individual with an inquiry or complaint may contact us using the mailing or email address below.

In the case of human resources data from the EU, NetForce has agreed to cooperate with a panel of European Data Protection Authorities created for that purpose. In the case of human resources data transferred from Switzerland, NetForce has agreed to cooperate with the Swiss Federal Data Protection and Information Commissioner.

In compliance with the Privacy Shield Principles, NetForce Global commits to resolve complaints about our collection or use of your personal information. EU and Swiss individuals with inquiries or complaints regarding our Privacy Shield policy should first contact NetForce Global by mail at: NetForce

Global LLC, 18 Crow Canyon Court, Suite 310, San Ramon, CA 94583 Attention Chief Compliance Officer or by email at: Joan.Grondin@netforceglobal.com.

If you have an unresolved privacy or data use concern with respect to data other than HR data that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider Truste at https://feedback-form.truste.com/watchdog/request. The services of Truste are provided at no cost to you.

Individuals also may be able to invoke binding arbitration, under certain circumstances where permitted by the Privacy Shield program, if the individual believes there has been a violation of Privacy Shield requirements that has not been appropriately addressed by NetForce Global.

NetForce Global's compliance with its Privacy Shield obligations also is subject to investigation and enforcement by the U.S. Federal Trade Commission. NetForce Global also is required by the Privacy Shield program to respond promptly to inquiries and requests for information from the U.S. Department of Commerce.

8. PUBLIC RECORD AND PUBLICLY AVAILABLE INFORMATION

In accordance with Privacy Shield, in cases where NetForce Global discloses public records or publicly available information from the EU and Switzerland without combining that information with non-public information, our general policies on Notice, Choice, and Accountability for Onward Transfer may not apply.

9. CONTACT US

In compliance with the Privacy Shield Principles, NetForce Global commits to resolve complaints about our collection or use of your personal information. EU and Swiss individuals with inquiries or complaints regarding our Privacy Shield policy should first contact NetForce Global by mail at: NetForce Global LLC, 18 Crow Canyon Court, Suite 310, San Ramon, CA 94583 Attention Chief Compliance Officer or by email at: Joan.Grondin@netforceglobal.com.

10. POLICY CHANGES

NetForce Global reserves the right to change their policy from time to time, consistent with the Privacy Shield Principles.