SUMMARY OF HEPE SECURITY MEASURES

To protect Customer data, HEPE abides by a robust set of information security controls including policies, practices, procedures, and organizational structures to safeguard the confidentiality, integrity, and availability of its own and its customers' information (including Personal Data as defined in HEPE's Customer and Data Processing Addenda). The following sets forth an overview of HEPE's technical/organizational security measures throughout the company.

1. Security Policy

HEPE maintains globally applicable policies, standards, and procedures intended to protect HEPE and Customer data. The detail of HEPE's security policies is confidential to protect the integrity of HEPE's data and systems. However, summaries of our key policies are included below.

2. Asset Management

HEPE has a process in place for identifying technical information assets, and through this process, HEPE identifies all assets under its responsibility and categorizes the critical assets. HEPE further maintains a set of documented handling procedures for each information classification type, including those assets that contain Personal Data.

Handling procedures address storage, transmission, communication, access, logging, retention, destruction, disposal, incident management, and breach notification.

3. Access Control

The principle of least privilege is used for providing logical access control. User access is provided via a unique user ID and password. HEPE's password policy has defined complexity, strength, validity, and password-history related controls. Access rights are reviewed periodically and revoked upon personnel departure.

User account creation and deletion procedures, as have been mutually agreed upon, are implemented to grant and revoke access to client systems used during the engagement.

4. Personnel Training

HEPE employees must complete the Integrity at HEPE training designed to ensure that employees are familiar with the program, policies, and resources that govern HEPE's expectations for ethical behavior, excellence, and compliance. Integrity at HEPE features modules on security and data privacy, and employees also are required to take an annual "refresher" course. HEPE employees must also complete an annually refreshed dedicated security awareness training focused on essential security policies and emphasizing the employees' responsibilities related to incident management, data privacy, and information security.

5. Third Parties and Subcontractors

HEPE has processes in place to select sub-contractors that are able to comply with comprehensive contractual security requirements.

For applicable suppliers (suppliers that handle/store/transmit HEPE data and customer owned HEPE held data or have

access to the HEPE network), HEPE Cybersecurity performs a risk assessment to verify the existence of an information security program. An adequate program must include physical, technical, and administrative safeguards. This assessment must be done before the supplier has access to HEPE information.

6. Systems Security

By policy, the development of systems and supporting software within HEPE follow a secure development methodology to ensure security throughout the system/software lifecycle. The Software Development Lifecycle defines initiation, development/acquisition, implementation, operations, and disposal requirements. All system components, including modules, libraries, services, and discrete components,are evaluated to determine their impact on the overall system security state.

HEPE has defined controls for the protection of application service transactions. These controls include validating and verifying user credentials, mandating digital signatures and encryption, implementing secure communication protocols, storing online transaction details on servers within the appropriate network security zone.

Internal vulnerability scans are performed regularly.

7. Cryptography

HEPE has defined a set of robust processes for cryptography to ensure the confidentiality, integrity, and availability of information assets. Approved protocols require encryption for certain assets, including those that contain personal data.

8. Business Continuity Management

HEPE maintains a global Continuity of Operations program. This program takes a holistic, company-wide approach

for end-to-end continuity through a set of collaborative, standardized, and internally documented planning processes.

HEPE periodically exercises its business continuity plans to ensure their effectiveness. HEPE currently tests and updates all plans at least yearly and ensures that people with a role in the business continuity plan are trained.

Revision Date	Brief Description of change	Revision Authority POC
November-2023	Initial Publication	Karina Rodriguez