**EXHIBIT B**

**THIRD PARTY SECURITY REQUIREMENTS**

# PURPOSE

All defined terms used in this Exhibit but not otherwise defined in this Exhibit shall have the meaning ascribed to such term in that certain Master Services Agreement, dated as of **\_\_\_\_\_\_\_\_\_\_\_**, 2020, by and between HNE and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (the “**MSA**”).

The purpose of this Exhibit is to prescribe the minimum data protection and information security standards that Contractor must meet and maintain during the Term. This Exhibit also provides the internal processes used by Contractor to mitigate risk associated with data security protocols.

During the course of providing Services under the Services Documents, Contractor may obtain, access or otherwise process, may be provided access to or otherwise obtain electronic data or information (including Covered Data) from or on behalf of HNE , or through an Authorized User’s use of the Services. Contractor shall protect all such data as detailed in this Exhibit.

# DEFINITIONS

For purposes of this Exhibit, the following definitions shall apply:

## “**Administrative User**”means a Representative that is designated and authorized by HNE to access and use the Services for administrative purposes.

## “**Agreement**” shall mean the MSA and all exhibits, schedules, attachments and appendices to the MSA.

## “**Authorized User**” means Administrative Users and End Users, as applicable.

## “**Applicable Laws and Regulations**” mean any applicable data protection, privacy or information security laws, codes and regulations or other binding restrictions applicable to Contractor, the provision of the Services, or the Processing of Covered Data that are applicable to or required by (i) the location(s) where Covered Data is Processed, (ii) the jurisdiction(s) in which Contractor or its sub-processors are located, or (iii) jurisdictions identified for an Authorized User.

## “**Covered Data**” means, for the purposes of this Exhibit, data or information (regardless of form, e.g., electronic, paper copy, etc.) that is:

### Confidential Information (including, for the avoidance of doubt, software source code and Protected Health Information, as that term is defined in HIPAA); and/or

### HNE Data or other data that, in each case, makes a natural person identified or identifiable or is a numerical, physical, physiological, cultural, economic, mental or other factor of identity relating to an identified or identifiable person (or other like term) under applicable data protection or privacy law and includes information that by itself or combined with other information can be used to identify a person.

## “**Data Centers**” means locations (including, without limitation, co-locations) at which Contractor provides Processing or data transmission functions in support of the Services Documents. Data Centers can be Contractor-owned or third-party service model-based.

## **“End User”** means a Representative (other than Administrative Users) who is designated and authorized by HNE to access and use the Services.

## “**Industry Recognized Framework**” means the HITRUST Common Security Framework, or a global industry recognized information security management system (“**ISMS**”) mutually agreed upon in writing by HNE and Contractor, such as ISMS standard *ISO/IEC 27001:2013 and ISO/IEC 27002:2013 – Information technology – Security techniques – Information security management systems – Requirements*, as published by the International Organization for Standardization and the International Electrotechnical Commission.

## “**Industry Standard Encryption Algorithms and Key Strengths**” means encryption that at least meets the following standard encryption algorithm (provided that the algorithm and key strengths may change depending upon the new and most up-to-date industry standard encryption practice):

### Transport Layer Security: TLS (≥ 256-bit);

### Advanced Encryption Standard: AES (≥ 256-bit);

### Asymmetric encryption: RSA (≥ 2048-bit); and

### Hashing: SHA-2 (≥ 224-bit) with “salt” shall be added to the input string prior to encoding to ensure that the same password text chosen by different Authorized Users will yield different encodings.

## “**Penetration Testing**” means the process for conducting an authorized simulated attack to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities, application flaws, improper configurations, or risky end-user behavior.

## “**Physical Security**” means the protection of facilities, systems, software, network and data from physical actions or unauthorized access through the use of multiple levels of security to ensure facilities remain secure and operational.

## “**Process**”, “**Processed**” and “**Processing**” means any operation or set of operations which is performed by Contractor upon Covered Data, whether by automatic means or not, including but not limited to collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, process, access, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

## “**Security Policies**” means established and maintained policies and procedures in support of data security (confidentiality, integrity and availability) across all systems, system interfaces, and business functions to prevent improper disclosure, alteration, or destruction of Covered Data.

# SECURITY MANAGEMENT

During the Term, Contractor shall maintain and enforce a written information privacy and security program (“**Security Program**”) that (i) complies with an Industry Recognized Framework, (ii) includes administrative, technical and physical safeguards reasonably designed to protect the confidentiality, integrity and availability of Covered Data, (iii) is appropriate to the nature, size and complexity of Contractor’s business operations, and (iv) complies with any Applicable Laws and Regulations.

## Security Program Changes. Contractor must have documented change management procedures in place for implementing changes to the production environment, including provisions for emergency changes, in accordance with industry best practices. Any change affecting Covered Data may be performed only if agreed to in writing by the Parties in accordance with Section 18 of the MSA.

## Training. Contractor shall certify that its Representatives will be provided with a clear understanding of procedures and controls reasonably necessary to comply with this Exhibit. Contractor’s Representatives will, upon hiring (within 90 days), and at least annually thereafter, participate in security awareness training. This training will cover, at a minimum, Contractor’s Security Policies, HNE ’s Security Policies, the requirements of this Exhibit, and any other topics requested by HNE , including acceptable use, password protection, data classification, social engineering, phishing and other internet fraud, training on application coding (where applicable), Security Incident reporting, the repercussions of violations, and brief overviews of Applicable Laws and Regulations. Contractor shall also provide training regarding data privacy and protection for Contractor’sRepresentatives Processing Covered Data as defined within this Exhibit.

## Subcontractor Due Diligence. To the extent subcontractors are permitted pursuant to the applicable terms and conditions of the MSA, Contractor shall maintain a security process to conduct appropriate due diligence prior to utilizing subcontractors to provide any of the Services. Contractor will assess the security capabilities of any such subcontractor on an annual basis to ensure such subcontractor’s ability to comply with this Exhibit, the other provisions in this Agreement, and the other Services Documents. The due diligence process will provide for the identification and resolution of significant security issues prior to engaging a subcontractor, written information security requirements that oblige subcontractor to adhere to Contractor’s key Security Policies, and identification and resolution of any security issues during the Term. Contractor shall be responsible for ensuring that subcontractors remediate any deficiencies found.

## Security Policies. Contractor shall maintain documented Security Policies to include the proper use of technologies, handling of Covered Data and appropriate safeguards. These Security Policies shall be provided and made available to all Contractor Representatives and subcontractors and, at a minimum, reviewed and updated on an annual basis.

## Identification of Point of Contact and Data Security Telephone Line. Contractor shall identify to HNE a senior employee as the point of contact responsible for overseeing and carrying out its Security Procedures and for communicating with HNE on information security matters during normal business hours. In addition, Contractor shall maintain a dedicated telephone line that will be answered by qualified data security personnel on a 24/7 basis. Any changes to the contact information in this Section 3(e) must be communicated to HNE at least forty-eight (48) hours prior to such change. Contractor shall periodically provide, at HNE ’s request, current information and documentation summarizing the Security Procedures, including documentation confirming that Contractor has satisfied its obligations under this Section 3(e).

# LOGICAL SECURITY

The logical security processes apply to the Services and supporting networks used to provide the Services on which Covered Data is Processed. Contractor shall use internal operational processes to keep the Covered Data secure and accessible to only authenticated Authorized Users of such Covered Data. Contractor shall also use Security Policies and access parameters denying direct access to Covered Data via direct file access and/or direct database access.

## Access Controls. Contractor certifies and warrants that it employs access control mechanisms that:

### prevent unauthorized access to Covered Data;

### limit access to Representatives with a business need to know;

### follow the principle of least privilege, allowing access to only the information and resources that are necessary under the terms of the Services Documents;

### have the capability of detecting, logging, and reporting access to the system or network or attempts to breach security of the system or networks; and

### prevent the use of default accounts and implement controls to prevent the sharing of accounts.

## Access Authorization. Contractor must have in place access controls for provisioning access to Authorized Users that support the Services. These access controls shall adhere to the following requirements, including without limitation:

### Contractor shall revoke Authorized User’s access to physical locations (Physical Security), systems, and applications that contain or Process Covered Data as soon as possible, but in any event no later than within twenty-four (24) hours of the cessation of such Authorized User’s need to access the system(s) or application(s).

### Contractor shall revoke Authorized User’s logical access (Logical Security), including remote access to systems, and applications that contain or Process Covered Data as soon as possible, but in any event no later than within twelve (12) hours of the cessation of such Authorized User’s need to access the system(s) or application(s).

### All Authorized Users must have an individual account that authenticates that individual’s access to Covered Data.

### Contractor must ensure that all passwords for applications that contain or Process Covered Data meet password requirements in accordance with HNE standards, which are as follows:

#### Must be at least eight (8) characters in length;

#### Username cannot be part of the password;

#### Lockout the user after five (5) unsuccessful logon attempts; and

### Passwords will be reset and delivered in a secure manner which includes removal, renaming, disabling, and/or changing all default usernames and default passwords.

### Contractor’s access privileges shall be recertified for End Users at least every six (6) months.

### Contractor’s access privileges shall be recertified for Administrative Users (e.g. system or security administrative authorities) and Contractor non-employee Authorized User accounts (e.g. service accounts) at least every ninety (90) days.

### Application development Authorized Users shall be restricted to no greater than read-only access for production data files or database tables. Technical controls shall be in place to prevent End User access to operating system resources.

### Contractor will provide HNE with a mechanism to view HNE Authorized Users and their access privileges, to the extent any such Authorized Users reside on Contractor systems.

## Regular Review of Access Controls. Contractor shall maintain a process to review access controls on an annual basis, at a minimum, for all Contractor’s systems that contain Covered Data, including any system that is used for any form of communication interface and can connect to the system on which Covered Data is Processed. These access processes and the process to establish and delete individual accounts will be documented in, and will be in compliance with, the Security Program.

## Secure Remote Access Authentication. Contractor shall configure secure remote access to all networks Processing Covered Data to require multi-factor authentication for such access by Contractor’s Representatives.

## Segmentation.Contractor shall strictly segregate Covered Data from information of Contractor or its other customers so that Covered Data is not logically or digitally commingled with any other types of information.

## Audit Logging. Contractor must enable system and application audit logging where technically possible. Contractor must retain logs for a minimum of twelve (12) months, and verify such logs periodically for completeness. Contractor shall make such logs available to HNE upon request. The following logging specifications must be included in the implementation of this requirement:

### Both successful and unsuccessful logon access attempts;

### Activities performed by Administrative Users with system or security administrator authorities;

### For network address management systems, all successful assignment and release of network IP address; and

### Date, time, user identifier, and type of access attempt or activity should accompany each audit log entry.

## Contractor shall monitor logs in near real time on a daily basis to look for evidence of misuse or authority using automated log monitoring software, and Contractor shall manually review logs at least once per month. Contractor shall escalate alerts and take action at the earliest opportunity following detection of misuse or authority.

# DATA SECURITY

## Contractor shall use Industry Standard Encryption Algorithms and Key Strengths that will ensure the confidentiality, availability and integrity of Covered Data hosted on Contractor systems. For both secret key and public/private key cryptography, Contractor must implement documented management procedures to manage the life cycle of the cryptographic keys including, without limitation, creation, distribution, validation, update, storage, usage, and expiration.

### Data Encryption in Transit. Contractor shall use Industry Standard Encryption Algorithms and Key Strengths for Covered Data while in transit over all public wired networks (e.g., Internet) and all wireless networks.

### Data Encryption at Rest. Contractor shall use Industry Standard Encryption Algorithms and Key Strengths for Covered Data at rest utilizing an industry recognized cryptography technology.

### Database Encryption. Contractor shall use Industry Standard Encryption Algorithms and Key Strengths for Covered Data residing in database systems utilizing an industry recognized cryptography technology.

### Data Backup Encryption. Contractor shall use Industry Standard Encryption Algorithms and Key Strengths for Covered Data residing on any production or archive systems or media utilizing an industry recognized cryptography technology.

### Mobile Devices. Contractor shall use Industry Standard Encryption Algorithms and Key Strengths for any mobile devices used outside of a Data Center (e.g., laptop, desktop tablet) hosting Covered Data to perform any part of the Services.

## Test Data. Unless otherwise authorized by HNE in writing, Contractor shall not use Covered Data for testing purposes unless the data has been de-identified or masked in accordance with all standards for de-identification set forth in Applicable Laws and Regulations, including, without limitation, the standards for de-identification of Protected Health Information (as that term is defined in HIPAA) set forth in HIPAA.

# NETWORK SECURITY

Contractor will follow industry best practices for its production network and related information security controls over any Covered Data transmitted using that network. Contractor agrees to implement network security controls, including without limitation:

## When creating a network connection to the Internet or with other third parties, Contractor must segment such networks and use a “defense in depth” approach with industry standard architectures (e.g., DMZ).

## With respect to Internet connections, Contractor must establish technical controls to protect against Distributed Denial of Service (“**DDoS**”) attacks.

## Data Loss Prevention (“**DLP**”) controls shall be in place to prevent Covered Data from being transferred to outside parties, including controls to prevent peer-to-peer sharing, instant messaging, or other Internet file sharing.

## All remote access to Contractor’s internal network must be done only through encrypted and secured means including the use of multifactor authentication.

## Contractor agrees to provide a high-level sanitized network diagram to HNE upon request.

## For any Internet-facing application with Covered Data, Contractor must implement a three-tier architecture design (e.g., at least two (2) firewalls or logical segregation configurations) to protect the application’s data tier, which should be clearly depicted on the aforementioned network map.

## Contractor must have a program in place to evaluate security patches and implement patches using a formal change process within the time limits specified below, along with provisions for applying emergency patches as necessary.

## Contractor must perform vulnerability scans semi-annually (twice per year) on all Internet-facing systems and on all other systems supporting HNE .

## Contractor must document identified vulnerabilities, risk ranked based on severity, and must take corrective action to correct such vulnerability as promptly as possible. Contractor shall provide HNE with copies of all such identified vulnerabilities as promptly as possible, and no later than five (5) business days after Contractor’s documentation of same. At any time, HNE can request evidence that identified vulnerabilities have been corrected, and Contractor shall promptly provide such evidence to HNE ’s satisfaction.

# SYSTEM SECURITY

## Anti-Virus/End Point and Anti-Malware Protection. Contractor shall maintain current versions of industry standard anti-virus/end point and anti-malware protection on all workstations, laptop and servers with the most recent updates available. Virus and malware definitions shall be updated within twenty-four (24) hours of release by the specific software or service vendor. Contractor shall configure this equipment and have supporting policies to prohibit users from disabling anti-virus and malware software, altering security configurations, or disabling other protective measures put in place to ensure the safety of Covered Data or Contractor’scomputing environment.

## Network Penetration Testing. Contractor shall conduct external network Penetration Testing either when a new component to the infrastructure is introduced or otherwise on an annual basis. Such Penetration Testing shall be performed using a certified Penetration Testing expert that is reputable in the industry.

## Vulnerability Management. Contractor shall run internal and external network vulnerability scans at least semi-annually (twice per year) and after any material change in the network configuration (e.g., new system component installations, changes in network topology, firewall rule modifications, or product upgrades).

## Patch Management. Contractor shall patch all workstations and servers with all current operating system, database and application patches deployed in Contractor’s computing environment according to a schedule predicated on the criticality of the patch. Contractor shall perform appropriate steps to help ensure patches do not compromise the security of the information resources being patched. All emergency or critical rated patches must be applied or have compensating and mitigating controls applied as soon as possible but at no time will exceed thirty (30) days from the date of release.

## System Hardening. Contractor shall conduct system hardening techniques on all hosts storing Covered Data. Hardening techniques at a minimum shall include various methods to secure application level, operating system level, system and BIOS level by keeping security patches and hot fixes up to date, disabling unnecessary ports and protocols, restricting local administrator accounts and applying security policies.

## Non-Production Environment. Unless specifically agreed upon and written approval is provided by HNE, at no time will Covered Data be Processed in a non-production environment.

## Incident Detection and Response. Contractor must have at least network- and preferably host-based Intrusion Detection Systems (“**IDS**”) and/or Intrusion Prevention Systems (“**IPS**”) in place and operational, which shall be updated regularly and monitored by Contractor. Procedures must be in place for Contractor to apply emergency IDS/IPS updates, as necessary. Contractor must have a clearly defined and documented escalation and communication process (internal and external), in the form of a Computer Security Incident Response Plan (“**CSIRT Plan**”), to be employed in the event of an incident. Such CSIRT Plan shall conform to best practices (NIST 800-61, ISO 27035) and shall include a Contractor point of contact that will be responsible for contacting HNE in the event of a Security Incident. Contractor shall test the CSIRT Plan at least annually (e.g. tabletop exercise) with testing details documented. Contractor will make both the CSIRT Plan and related testing available to HNE upon request.

# ASSET MANAGEMENT

## Asset Management. Contractor shall adhere to the following asset management requirements, including, without limitation:

### An Asset Management Policy must be defined in accordance with industry best practices, and must include, without limitation, asset classification (e.g. information, software, hardware).

### All Contractor physical assets, if any, must be clearly labeled as to ownership and inventoried in a manner commensurate with industry best practices.

### All Covered Data must be labeled as to classification.

### Appropriate physical controls must be in place to prevent unauthorized access to hard copy output containing Covered Data.

### Contractor must periodically reconcile and account for all physical assets (e.g. laptops, mobile devices), if any are in possession of Contractor and/or its Representatives and all storage media containing Covered Data, at least annually.

### Contractor must have procedures in place to ensure termination or change in employment of its Representatives results in prompt return of physical assets, if any are assigned to said Representatives, and removal of access rights are completed in accordance with Section 4(b).

### Removable storage media containing Covered Data must be encrypted pursuant to Section 5, marked accordingly whenever possible, and stored in a locked container in transit and in a controlled access area while on Contractor premises.

### Movement of storage media to and from an authorized media retention facility must be accounted for using a secured carrier with transmittal records in accordance with industry best practices.

### Contractor must report a Security Incident in accordance with Section 5.6(f) of the MSA in the event storage media containing Covered Data is determined to be missing, lost, or otherwise unaccounted for as a result of inventory reconciliation activities.

## Mobile Devices. If Contractor allows its Representatives to use a personal mobile device (e.g. Bring Your Own Device, or BYOD) in order to access Covered Data, then in addition to all other requirements set forth in this Exhibit, Contractor must also have Mobile Device Management (“**MDM**”) controls, which includes, without limitation:

### A Personal Identification Number or passcode policy in order to unlock the device.

### Full encryption of the mobile device using technologies pursuant to Section 5.

### Function for remotely locking and wiping the device of all data, even if it means deleting personal information from the device.

### Function for revoking privileges to Covered Data if the device is rooted, jail broken, or out of compliance with the MDM policy.

# EMAIL SECURITY

## If Contractor sends an email to HNE or a third party which addresses or includes Covered Data, it must use appropriate email identity solutions, including but not limited to DKIM, SPF, and DMARC. If Contractor uses Authorized User-owned domain names to send emails, Contractor shall adhere to such Authorized User’s email security requirements, provided upon request.

## If Contractor allows its Representatives to remotely access email (e.g., use a webmail client interface, use personal devices on Contractor networks, access Contractor email remotely) then proper security measures must be taken to ensure Covered Data does not leave the confines of the Contractor network (e.g. using a DLP solution to block Covered Data being stored or copied to an unauthorized service and/or device). Contractor shall prevent the transmission of Covered Data to computers that are not under Contractor’s control, such as shared computers or hotel business centers.

# SERVICES SECURITY

## Security Assessments. For all Internet-facing applications that Process or display Covered Data, Contractor shall conduct an application security assessment review to identify common security vulnerabilities as identified by industry-recognized organizations (e.g., OWASP Top 10 Vulnerabilities; CWE/SANS Top 25 vulnerabilities) annually or for all major releases, whichever occurs first. The scope of the security assessment will primarily focus on application security, including, but not limited to, Penetration Testing of the application, as well as a code review. At a minimum, it will cover the OWASP Top 10 vulnerabilities (https://www.owasp.org).

## Web Application Firewall/DoS/DDoS Protection. Contractor shall deploy reasonably appropriate web application firewall technology in the operation of protecting Contractor’s web applications. Web application firewall at a minimum shall protect protocol traffic and services at OSI layers 3, 4, 5 and 7.

## Data Encryption. Contractor shall deploy Industry Standard Encryption Algorithms and Key Strengths for both Contractor Web applications and Contractor Mobile applications utilizing the HTTPS protocol in a request-response architecture utilizing the latest secure version of TLS certificate verified by industry recognized certificate authority.

## Single Sign-On Integration. If available as part of Contractor’s Services and if procured by Authorized User, integration of Security Assertion Markup Language (SAML) shall be configured where possible utilizing Authorized User’s Single Sign-On (SSO) platform. If SAML integration is not available Contractor may provide an alternative Single Sign-On technology, e.g., Azure Active Director, OAuth (Open Authorization). For clarity, as of the Effective Date, SSO services are not part of Contractor’s Services.

# DATA CENTER AND PHYSICAL SECURITY

## Location of Data Centers. Contractor shall (i) provide a current list of the Data Centers and (ii) notify HNE if it adds or removes a Data Center at least fourteen (14) days prior to adding or removing such Data Center. The Data Centers as of the Effective Date are set forth below:

|  |  |
| --- | --- |
| Entity Name | Corporate Location |
|  |  |
|  |  |
|  |  |

## Physical and Environmental Controls for Data Centers. Contractor shall physically locate Data Centers in controlled access areas. The following specifications shall apply to all Data Centers and must be included in the implementation of this Section 11:

### Entry into controlled access areas must be prohibited from building areas that are open to the general public.

### The controlled access area must be locked, even when attended.

### Slab-to-slab barriers or intrusion detection must be used to deter unauthorized access to the area.

### Access to the area must be through a dual entry system, in which access to the second door is only granted upon the first door being locked.

### Only authorized persons may enter the area and access authorization procedures must be defined and implemented.

### Persons with authorized access must have a current business requirement for the access from the area owner, who is expected to make the determination of what constitutes a business requirement and be able to demonstrate that such a determination was made.

### Physical access control mechanisms must electronically record access to the area.

### Cameras that have the ability to provide alerting capabilities with clear visibility of individual faces.

### The area’s authorized access list must be verified and signed (hard copy or electronic) by the area owner at least every three (3) months.

### Persons who have had their access authorization revoked, either by request or implicitly through termination of employment, must be removed from the access list as set forth in Section 4(b)(i).

### An accurate, current log of non-routine accesses must be kept which reflects the visitor name, time/date of entry, the authorized escort, and the fact of exit, with the purpose of the log being to provide a historical record of access rather than a control tool.

### Emergency exits must have working, audible, and monitored alarms that operate on emergency power with all alarm events initiating investigative action.

### Emergency exit alarms must be tested periodically to verify that they are functioning with test results documented.

### A water identification system (e.g., halon like sprinklers) must be used.

### The area must have appropriate ventilation and appropriate uninterrupted power supply (e.g., generators).

### LAN management systems, wireless access points, and other small servers must be located in a locked area when unattended.

## Multitenant Hosting. “**Multitenant Hosting**” means any shared computing environment in which infrastructure and computational resources support two (2) or more organizations, such that the software application and database design handles the logical separation of Covered Data. To the extent that Covered Data is Processed in a Multitenant Hosting environment, Contractor shall implement and maintain the Multitenant Hosting controls set forth in this Section 11(b):

### Logical isolation of Covered Data to prevent the Covered Data from viewing or other access by other tenants sharing the environment.

### Strong management practices to ensure that the controls developed to maintain isolation are not circumvented or otherwise modified.

### Periodic tests, no less than annually, to verify that the controls in place to manage the isolation of Covered Data have not been altered in a way that reduces the effectiveness of the controls or otherwise confirms that a degradation of the controls has not taken place over time. Results of such testing will be made available to HNE upon request.

### System and application data that is backed up from the Multitenant Hosting environment will retain similar access controls found within the application that restrict what data can be viewed or accessed by tenants including their employees and agents.

### Any data that is extracted from the system (e.g. to provide information to one of the tenants) will be verified by Contractor prior to sending the information to the tenant that only the applicable tenant’s information is provided. Contractor will ensure that Covered Data is not included within data files provided to fulfill requests from other Multitenant Hosting tenants.

### The unique code or combination of fields that are designed to represent HNE may not have been used in the past to identify a prior tenant. Similarly, if HNE terminates the Services, the unique code or combination of fields that are used to identify HNE may not be reused in the future to designate a new tenant.

### Robust access controls that enforce isolation of each tenant’s data which provides the following features:

#### Controls in place restrict access to data within each tenant’s environment.

#### Designated tenant administrators for the other parties within the Multitenant Hosting environment must be prevented from elevating their access in a way that would permit the tenant administrator to access Covered Data.

#### Changes to the systems or programs that manage the access controls that isolate Covered Data from other tenants must be tested prior to implementing any changes within the Multitenant Hosting environment such that isolation controls are verified and are not compromised by the changes.

## Cloud Computing.

### “**Cloud Computing**” means any shared computing environment in which a set of systems and processes act together to provide services in a manner that is disassociated with the underlying specific hardware or software used for such purpose. To the extent that Covered Data is Processed in a Cloud Computing environment, Contractor shall implement and maintain Cloud Computing controls per the defined subtypes below:

#### “**Private Cloud**” means the provision of computing capabilities as a service and use thereof either by a single organization or by multiple organizations that can use the same services (including infrastructure, platform, and/or software) in an architecture, configuration, and/or system that ensure that one organization’s use and data are completely isolated from uses and data of other organizations.

#### “**Public Cloud**” means the provision of computing capabilities as a service to external customers using Internet technologies. Public Cloud computing uses cloud computing technologies to support customers that are external to the provider’s organization. When using Public Cloud services, any organization (in any industry sector and jurisdiction) can use the same services (including infrastructure, platform, and/or software), without guarantees about where data will be located and stored.

#### “**Hybrid Cloud**” means a combination of Public Cloud and Private Cloud solutions.

## Contractor shall not Process Covered Data on a Public Cloud or on the Public Cloud portion of a Hybrid Cloud solution, nor store Covered Data on a Public Cloud or on the Public Cloud portion of a Hybrid Cloud solution unless encryption is used in both transit and at rest pursuant to Section 5. For all Cloud Computing environments, Contractor shall validate compliance at least annually with either (a) the latest version of the Cloud Security Alliance Cloud Controls Matrix, (b) Federal Risk and Authorization Management Program compliance, or (c) a HNE-approved equivalent set of security, privacy, and business continuity controls, which will meet HNE’s external and internal compliance requirements for protecting Covered Data.

# APPLICATION CODING

## To the extent Services involve application coding commissioned by HNE both directly and specifically for the benefit of HNE (e.g., application development, application maintenance), Contractor shall adhere to the application coding commitments provided herein.

## Application Vulnerability Testing. Contractor shall perform Application Vulnerability Testing (“**AVT**”) annually as part of the AVT program. The AVT program is established to identify and remediate/fix Internet-facing vulnerabilities to protect HNE from a potential risk of data loss and/or breach of security. Contractor shall work with HNE during the AVT process, including, without limitation:

### Using a combination of scanning platforms and Contractor providers to identify vulnerabilities in code/modules created by Contractor, both pre- and post-production, on an annual basis or at a frequency otherwise determined by HNE.

### Contractor shall be responsible for remediating all vulnerabilities identified by third-party testers to HNE’s satisfaction at no additional cost to HNE prior to the release of the code into production or within 90 days of identification of the vulnerability. HNE may, in its sole discretion, run additional tests after each vulnerability fix performed by Contractor to validate each identified vulnerability is fixed to HNE ’s satisfaction and industry standards, and will be subject to HNE ’s acceptance.

### In the event code enters production without completion of the AVT program and/or otherwise through routine scanning, Contractor’s responsibility to remediate does not end upon acceptance of the code by HNE. For avoidance of doubt, as described above, if vulnerabilities are identified after HNE’s initial acceptance of the application code, prior to the independent AVT program commencement, all remediation rework will be at no additional cost to HNE provided these issues are formally identified by HNE within six (6) months after code goes into production.

# DATA RETENTION AND DESTRUCTION

## Data Access and Retention. In accordance with Applicable Laws and Regulations, Contractor shall retain all Covered Data in accordance with Section 2.3 of the MSA.

## Data Destruction. Contractor shall dispose of Covered Data in accordance with the procedure and timeframes set forth in Section 6.4(b) of the MSA. Contractor shall cooperate fully with HNE’s reasonable requests for access to, correction of, and destruction of Covered Data in Contractor’s possession, which shall be certified to HNE in writing. Covered Data must be made unrecoverable upon disposal. Contractor must ensure that all storage media being disposed of containing Covered Data is sanitized in accordance with NIST Special Publication 800-88, DoD 5220.22-M “Cleaning and Sanitizing Matrix,” or equivalent practices. Additionally, any decommissioned hardware containing Covered Data must be destroyed by a third party that issues a certificate of destruction upon disposal.

# BUSINESS CONTINUITY AND DISASTER RECOVERY

## Business Continuity. “**Business Continuity**” means a set of planning, preparatory, and business process controls which are intended to ensure either the continuation or prompt recovery of critical business functions despite serious incidents or disasters that might have interrupted them. Contractor shall adhere to Business Continuity requirements reasonably acceptable to HNE, including, without limitation:

### Contractor shall ensure the integrity of its business by having in place capacity planning, change management, and project management disciplines that are integrated with the Business Continuity Plan (“**BCP**”), with a duly authorized member of senior management who is suitably qualified in Business Continuity planning, and who shall be responsible for the development, maintenance, management, and exercising of the BCP.

### Contractor shall complete an annual risk assessment and business impact analysis to address a range of plausible threats, together with an assessment of the associated impacts and probabilities. Contractor will align the business process priorities from the risk assessment and ensure that all critical processes will be recovered irrespective of any event, the results of which will be a formally documented, regularly maintained BCP that meets or exceeds best practices (e.g. NIST SP800-34, ISO 22301).

### The business impact analysis driving the level of content within the BCP shall include these requirements:

#### Critical upstream and downstream processes;

#### Minimum Recovery Point Objective, as set forth in the Statement of Work (“**RPO**”);

#### Maximum Recovery Time Objective, as set forth in the Statement of Work (“**RTO**”); and

#### Critical business resource requirements for recovery over time period, including without limitation:

##### Skill resources;

##### IT systems/applications;

##### Telephony requirements; and

##### Endpoint hardware (e.g., desktops, laptops).

### Contractor shall have provisions in place for maintaining contact details of its Representatives and relevant HNE Representatives, and these contacts shall be periodically audited for accuracy. Contractor will promptly notify HNE of any disruption in service that exceeds the RTO.

### Contractor shall at all times have qualified and trained personnel, including backup personnel for all key positions who are empowered to make decisions to ensure prompt business recovery.

### Any alternative workplace recovery centers required for the performance of Services shall meet Contractor’s resource requirements and sited no more than twenty-five (25) miles (on a straight-line basis) from the Contractor facility being covered with a distance not more than can reasonably be expected to travel in ninety (90) minutes. Contractor shall have appropriate and binding contracts in place for the use of any such workplace recovery centers. Contractor may permit remote access in lieu of workplace recovery centers provided that remote access to Contractor’s internal network is encrypted and secured using multifactor authentication.

### Contractor shall update its BCP at least annually using industry best practices, and within thirty (30) calendar days of any significant changes to the business. For example, the closure/exit of a facility used to support Services would require an update to the BCP.

### Contractor shall ensure that both critical and non-critical Business Continuity exercises and validation is an integral part of the Business Continuity management process and shall document and validate such exercises at least once per year. Additionally, Contractor shall conduct exercises on any recently updated portions of the BCP, and Contractor shall conduct an exercise of the BCP within forty-five (45) days of any failure.

### Contractor shall ensure that all of these BCP requirements are communicated to and implemented by its third-party providers. A copy of the BCP will be made available to HNE upon request. Contractor shall provide HNE with copies of all updates to the BCP as promptly as possible, and no later than five (5) business days after its adoption by Contractor. Contractor shall provide HNE with copies of all exercise schedules, and copies of executive reports and summaries resulting from any exercise results, in each case as promptly as possible, and no later than five (5) business days after Contractor’s receipt or preparation thereof.

### Contractor shall implement the BCP in the event of any unplanned interruption of the Services.

## Disaster Recovery. “**Disaster Recovery**” means a set of policies, procedures, and technical controls designed and operating to enable the recovery or continuation of technology infrastructure and systems following any natural or human- induced disaster. Contractor shall adhere to Disaster Recovery requirements reasonably acceptable to HNE, including, without limitation:

### Contractor shall ensure the integrity of the business by having in place capacity planning, change management, and project management disciplines that are integrated with a Disaster Recovery Plan (“**DRP**”).

### Contractor’s Disaster Recovery program shall be overseen by a duly authorized member of senior management who is suitably qualified in Disaster Recovery planning, and who shall be responsible for the development, maintenance, management, and testing of the DRP.

### Contractor shall complete an annual risk assessment and determine any significant single points of failure in systems used to provide Services. Contractor shall ensure that the IT requirements to support the provision of Services are adequate with no single points of failure and/or appropriate recovery procedures in a formally documented, regularly maintained DRP that meets or exceeds best practices (NIST SP800-34, ISO 24762, ISO 22301).

### Contractor shall provide and/or procure for the provision of appropriate Disaster Recovery planning from the Effective Date to ensure that all Services are operational after any risk event within the relevant RTO and data restored to the relevant RPO, as set out in any applicable Services Documents.

### Contractor shall provide and maintain sufficient Disaster Recovery datacenters and associated recovery facilities to be used in an invocation so that the RTO can be met. Unless otherwise agreed with HNE , any Disaster Recovery datacenter shall be sited at least one hundred (100) miles (on a straight-line basis) from and service by a separate utility than the primary datacenter. Contractor should maintain redundancy of all equipment between these facilities, including redundant contracts with subcontractors designed to lessen residual dependency (e.g. redundant fuel delivery contracts). In addition to redundant contracts, Contractor will ensure that sufficient funds and resources are available at all times in order to ensure the efficient and uninterrupted management of the required DRP.

### Contractor shall ensure that Disaster Recovery is supported with appropriate data replication and backups both onsite and offsite. These will be of a frequency and concurrency to meet RPO and RTO commitments.

### Contractor shall backup Covered Data to ensure that RPO can be met. Backed up data will be either transported offsite or securely copied to secondary secure devices and Disaster Recovery datacenters so long as the method used meets RPO commitments. Any backup copy of Covered Data at any Disaster Recovery datacenter shall be stored in encrypted format pursuant to Section 5.

### Contractor shall monitor replication to ensure backups are appropriately performed and backed up data is complete in nature. Contractor shall promptly report to HNE all failures in replication or backups to complete or to be sent offsite.

### Contractor shall update the DRP at least annually using industry best practices, to ensure every point of failure is appropriately documented in the DRP. Additionally, an update of the DRP is required within thirty (30) calendar days of significant changes to the business, IT systems, and/or infrastructure. For example, change of a datacenter site would result in an update to the DRP.

### Contractor shall ensure that both critical and non-critical testing and validation is an integral part of the Disaster Recovery management process and will have provisions for documented annualized testing and validation. Additionally, Contractor shall test any recently updated portions of the DRP within thirty (30) calendar days of such change and within forty-five (45) days of a failure. The elements of each test plan shall include, without limitation:

#### Incident scenario;

#### Scope and objectives;

#### Approach;

#### Success criteria; and

#### Assumptions and exceptions.

### Contractor shall ensure that the DRP is readily available to its Representatives with roles and privileges appropriate for both recovering functions and in the performance of Services from unplanned disruptions per the DRP.

### Contractor shall ensure that the technical detail in the DRP is written clearly and unambiguously such that the DRP can be understood and implemented by appropriately trained personnel, to whom the DRP will be made available. A copy of the DRP will be made available to HNE upon request. Contractor shall provide HNE with copies of all updates to the DRP as promptly as possible, and no later than five (5) business days after its adoption by Contractor. Contractor shall provide HNE with copies of all DRP testing schedules, and copies of executive reports and summaries resulting from such testing, in each case as promptly as possible, and no later than five (5) business days after Contractor’s receipt or preparation thereof.

### Contractor shall implement the DRP in the event of any unplanned interruption of the Services.

# RISK ASSESSMENT PROCESS.

Contractor shall comply with HNE’s risk assessment requirements, including assessment prior to performance of Services and periodic recertifications or reassessments, which may occur no more frequently than once annually unless there is a Security Incident or of the provisions herein. As part of such assessment and recertification, Contractor shall certify compliance with all pertinent HNE IT policies and standards through performance of the risk assessment process, which includes, without limitation:

## Promptly complete risk assessment questionnaires as provided to Contractor in writing by HNE.

## Promptly provide copies or otherwise make available for review all supporting documentation to risk assessment questionnaire responses as reasonably requested by HNE.

## Allow HNE to verify environmental and physical security controls at all Contractor IT and business facilities where Covered Data is processed.

## Remediate any and all issues identified through the risk assessment process in a timely manner commensurate with the risk and consistent with healthcare industry best practices and standards.