14. **Data Access and Security/Payment Card Industry Data Security (PCI DSS) Compliance.**
    - 14.1 **Accessing Data -** While providing services, [company name] may be required to access, receive, transmit or maintain financial or business data or personally identifiable information from or on behalf of USNH or its students, employees, or agents. Any data that [company name] accesses, receives, transmits or maintains (collectively, "USNH Data") shall be treated as confidential and protected as stated in this section.
    - 14.2 **Compliance with Laws** – [company name] agrees to comply with all applicable federal, state and local laws, regulations and rules, and when applicable, the European Union's General Data Protection Regulation 2016/679, in connection with its access to or handling of USNH Data.
    - 14.3 **Data Return or Destruction**:
        - 14.3.1 Unless directed to return the USNH Data to USNH, [company name], its subcontractors and agents, shall Securely Destroy all USNH Data in their possession and within 60 days of termination of the contract. [company name] agrees to provide reasonable documentation of such data destruction to USNH.
        - 14.3.2 "Securely Destroy" means taking actions which meet or exceed the National Institute of Standards and Technology (NIST) SP 800-88 guidelines, or other similar industry accepted standards, relevant to data categorized as high security to render data written on physical (e.g., hardcopy, microfiche, etc.) or electronic media unrecoverable by both ordinary and extraordinary means.
    - 14.4 **Security Assessments**
        - 14.4.1 [company name] will satisfy the requirements of the USNH security assessment review (SAR), or specific USNH campus equivalent.
        - 14.4.2 USNH shall have the right, no more than once annually, upon reasonable prior notice, to review [company name]'s compliance with these requirements and its security measures relating to USNH Data, including the right to have an independent third party conduct a data security audit. [company name] and USNH shall work in good faith to determine the scope and time for performance of such audits to minimize disruptions to [company name]'s business operations and allow [company name] to maintain reasonable control over access to and security of its infrastructure and audit artifacts. Audits shall be limited to those facilities, systems and information material to the services provided USNH by [company name].
    - 14.5 **Information Security**
        - 14.5.1 [company name] agrees to implement administrative, physical and technical safeguards to protect USNH Data that meet accepted industry practices.
        - 14.5.2 [company name]'s safeguards to protect USNH Data shall include:
            - 14.5.2.1 securing business facilities, data centers, paper files, servers, back-up systems and computing equipment, including all mobile devices and other equipment with information storage capability
            - 14.5.2.2 implementing network, device, application, database and platform security
            - 14.5.2.3 securing information transmission, storage and disposal
            - 14.5.2.4 implementing authentication and access controls within media, applications, operating systems and equipment, leveraging USNH authentication services as applicable
            - 14.5.2.5 encrypting USNH Data at rest or in transit
            - 14.5.2.6 segregating USNH Data from [company name]'s or its other customers' information
            - 14.5.2.7 implementing appropriate personnel security and integrity procedures and practices, including background checks

14.5.2.8 providing appropriate privacy and information security training to [company name]'s employees

14.6 **Payment Card Standards**

14.6.1 To the extent [company name] collects or has access to any information involving payment card data under the contract, [company name] shall adhere to all applicable payment card industry requirements, including, the current Payment Card Industry Data Security Standard (PCI DSS).

14.6.2 [company name] is solely responsible for the protection and security of any cardholder data that [company name] possesses, stores, processes, or transmits on behalf of USNH.

14.6.3 [company name] is also responsible for its actions or inactions concerning payment card security to the extent that they could impact the security of the customer's cardholder data environment.

14.6.4 [company name] must provide proof of compliance in the form of a processor provided certificate with the current PCI DSS on an annual basis. Acceptable proof will be an Attestation of Compliance, appropriate to the [company name]'s PCI DSS compliance level, properly completed, and less than twelve months old. For example, a Level 1 company would be required to deliver the Attestation of Compliance from a QSA-led Onsite Assessment (also known as a PCI Report on Compliance, ROC). Companies eligible to self-assess should provide an AOC signed by an authorized executive of the company. This AOC would ideally be supported by a Qualified Security Assessor (QSA as defined in the PCI DSS) signature, but it is not required.

14.7 **Security Incident Response Protocols**

14.7.1 Immediately upon execution of the contract, [company name] shall provide to the USNH and the campus Information Technology contacts the name and contact information of [company name]'s employee who shall serve as USNH's primary security contact and shall be available to assist USNH within 4 hours of discovery of a breach and be available to resolve obligations associated with a security breach.14.7.2 In the event of an information security incident involving the security, confidentiality, integrity, and/or availability of USNH Data or in which USNH Data could have been compromised or subject to unauthorized access (a "Security Incident") the following steps will be taken:

14.7.2.1 U*SNH & Campus Notification* - [company name] shall immediately notify the USNH and the campus IT contact as soon as practicable but no later than 24 hours after [company name] becomes aware of the Security Incident. The USNH notice shall be sent by email with a read receipt requested to IT.Security@unh.edu. The campus email notice shall be sent to the current contact.

14.7.2.2 *Investigation* - Immediately following [company name]'s notification to USNH of a Security Incident, the parties shall coordinate to investigate the Security Incident. [company name] agrees to reasonably cooperate with USNH in handling the Security Incident, including (i) assisting with any investigation; (ii) upon request, provide USNH with physical access to the facilities and operations relevant to the USNH Data affected; (iii) upon request, facilitating interviews with [company name]'s employees and others involved in the Security Incident; and (iv) making available all relevant records, logs, files, data reporting and other materials relating to the Security Incident required to comply with applicable laws, regulations, or as

otherwise reasonably required by USNH; (iv) provide assistance and notification if the breach is the result of a 3d parties contractor or supply chains; (v) vendor will be responsible for the costs of notification and credit monitoring if they cause the breach.

14.7.2.3 *Notification to Third Parties* – Except as required by law, [company name] agrees that it shall not inform any third party of any loss or compromise of any USNH Data without first obtaining USNH's written consent, other than to inform a complainant that notice of the Security Incident has been forwarded to USNH's legal counsel. Further, [company name] agrees that USNH shall have the sole right to determine: (i) whether notice of any loss or compromise of USNH Data is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation; and (ii) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.

14.7.2.4 *Remedy of Vulnerability and/or Exploitable State*– [company name] shall use reasonable efforts to immediately remedy any security vulnerabilities and/or exploitable states to mitigate potential damage or loss during an ongoing security incident in accordance with applicable privacy rights, laws, and regulations "Reasonable efforts" means, with respect to this requirement, the efforts that a reasonable person in [company name]'s position would use to comply with this obligation as promptly as possible.

14.7.2.5 C*ost of Breach* - [company name] shall be responsible for all costs associated with any Security Incident. [company name] shall reimburse USNH for actual costs incurred by USNH in responding to, and mitigating damages caused by, any Security Incident, including (i) all costs of notice and/or remediation and any fees imposed by regulatory agencies, contracting partners, or other entities resulting from the Security Incident or (ii) providing notification to individuals whose Personally Identifiable Information was compromised.