DATA PRIVACY AND SECURITY
TERMS AND CONDITIONS

The following terms and conditions, as applicable to the services and/or goods being provided to Tennessee Tech, shall govern the use of Personal Information by the parties.

Data Privacy:

a) Definition of Personal Information.

For the purposes of this section, "Personal Information" means information provided to Contractor by or at the direction of University, or to which access was provided to Contractor by or at the direction of University, in the course of Contractor's performance under this Agreement that: (i) identifies or can be used to identify an individual including, without limitation , names, signatures, addresses, telephone numbers, e-mail addresses and other unique identifiers; or (ii) can be used to authenticate an individual including, without limitation, employee identification numbers, government-issued identification numbers, passwords or PINs, financial account numbers, credit report information, biometric or health data, answers to security questions and other personal identifiers. Where applicable, "Personal Information" may also mean any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

b) Protection of Personal Information.

i) Personal Information Protected by HIPAA.

To the extent required by federal law, the Parties agree to comply with the Health Insurance Portability and Accountability Act of 1996, as codified at 42 U.S.C. Section 1320d ("HIPAA") and any current and future regulations promulgated thereunder, including without limitation, the federal privacy regulations, the federal security standards, and the federal standards for electronic transactions, all collectively referred to herein as "HIPAA Requirements." The Parties agree not to use or further disclose any Protected Health Information or Individually Identifiable Health Information, other than as permitted by HIPAA Requirements and the terms of this Agreement.

ii) Personal Information Protected by FERPA.

Contractor agrees that to the extent it receives any personally identifiable information or information that could lead to personally identifiable information about students, Contractor will protect the privacy of all student education records to the full extent required of University under the Family Educational Rights and Privacy Act ("FERPA") (20 U.S.C. § 1232g; 34 CFR Part 99).

Because Contractor is performing an institutional service or function that has been outsourced by University and for which University would otherwise use its employees and is under the direct control of University with respect to the use of the education records, as defined by FERPA, Contractor recognizes it is subject to all FERPA requirements governing the use and redisclosure of personally identifiable information from education records, including without limitation the requirements of 34 CFR §99.33(a). Furthermore, Contractor may not disclose or redisclose personally identifiable information unless University has first authorized in writing such disclosure or redisclosure; will not use any personally identifiable information acquired from University for any purpose other than

performing the service or function that is the subject of this Agreement; and agrees to return to University (or, if not feasible, to securely destroy) education records in whatever form or medium that Contractor received such records from or created them on behalf of University.

iii) Personal Information Protected by GLBA, FTC Red Flags Rule, and Other Privacy Laws.

Contractor agrees to implement and maintain a written comprehensive information security program containing administrative, technical and physical safeguards for the security and protection of applicable Personal Information in compliance with the Gramm-Leach-Bliley Act ("GLBA")(15 U.S.C. § 6801; 16 CFR Part 314) and the Federal Trade Commission's Red Flags Rule (15 U.S.C. § 1681; 16 CFR Part 681). Upon University's request, Contractor shall provide evidence that is satisfactory to University of its information security program.

iv. Personal Information Protected by the GDPR.

1) Tennessee Tech collects the information Contractor provides to it for the purpose fulfilling its obligations under this contract. Tennessee Tech will share the information Contractor provides only to the extent required by law.

   Tennessee Tech will store Contractor's personal data consistent with its policies on document retention, which can be accessed through this link: https://www.tntech.edu/policies/.

   If Contractor is a resident of the European Economic Area ("EEA") and has standing under the General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, Contractor may have the right (i) to request from Tennessee Tech access to and rectification or erasure of personal data or restriction of processing; (ii) to object to processing; (iii) to data portability and (iv) to lodge a complaint with a supervisory authority in the EEA.

   By providing personal data to Tennessee Tech, Contractor consents to the processing of your data for the purposes described above.

2) See attached GDPR Data Protection Addendum for additional GDPR requirements, if applicable.

c) Return of Personal Information.

At any time during the term of this Agreement, at University's written request or upon the termination or expiration of this Agreement, Contractor shall return to University all copies, whether in written, electronic or other form or media, of Personal Information in its possession, or at University's direction, securely dispose of all such copies.

d) PCI-DSS.

The Contractor agrees to comply with the provisions outlined in the Payment Card Industry Data Security Standard (PCI DSS) and adhere to the merchant level vulnerability testing.

I. Data Security.

Contractor represents and warrants that its collection, access, use, storage, disposal and disclosure of Personal Information complies with all applicable federal and state privacy and data protection laws.

SOCII / SOCIII / SSAE 18.

1) Data Security Controls

Contractor represents and warrants that Contractor will maintain compliance with SSAE-16 or -18 SOC Type I, II, or III standards, and shall undertake any audits and risk assessments Contractor deems necessary to maintain compliance with the same.

2) **Reporting on Data Security Controls**

At University's request, Contractor will provide assurances to University that are acceptable to University related to Contractor's organization controls surrounding all systems and data related to this Agreement. Such assurances may include, but are not limited to, SSAE-16 or -18 SOC Type I, II, or III reports or any other reports in a form requested by University or required by applicable data protection laws.

a) Security Incident Response.

1) Definition

"Security Incident" means any breach or reasonably suspected breach of information system(s), including but not limited to unauthorized access to any system, server or database, or any other unauthorized access, use, or disclosure of information occurring on system(s) under Contractor's control.

Contractor's Responsibilities

a. Contractor shall:

(i) Provide University with the name and contact information for an employee of Contractor who shall serve as University's primary security contact and shall be available to assist University twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a Security Incident;

(ii) Notify University of a Security Incident as soon as practicable, but no later than forty-eight (48) hours after Contractor becomes aware of it, except where disclosure is prohibited by law;

(iii) Notify University of any such Security Incident by email to ociso@tntech.edu with a copy by email to Contractor's primary University business contact;

(iv) Contractor shall use best efforts to immediately mitigate or resolve any Security Incident, at Contractor's expense and in accordance with applicable privacy rights, laws, regulations and standards; and

(v) Take any and all such actions that a prudent Contractor would take in light of the circumstances and severity of the Security Incident.

b) Liability for Costs Related to a Security Incident

Contractor shall reimburse University for damages and actual costs incurred by University in responding to, and mitigating damages caused by any Security Incident, including all costs of notice and/or remediation incurred under all applicable laws as a result of the Security Incident.

c) Cyber Insurance.

Contractor shall carry error & omissions and cyber liability insurance in an amount not less than $5,000,000 per claim and annual aggregate, covering all acts, errors, omissions, negligence, infringement of intellectual property (except patent and trade secret); network security and privacy risks, including but not limited to unauthorized access, failure of security, breach of privacy perils, wrongful disclosure, collection, or other negligence in the handling of confidential information, privacy perils, and including coverage for related regulatory defense and penalties; data breach expenses, in an amount not less than $5,000,000 and payable whether incurred by University or Contractor, including but not limited to consumer notification, whether or not required by law, computer forensic investigations, public relations and crisis management firm fees, credit file or identity monitoring or remediation services in the performance of services for University or on behalf of University hereunder.