DATA PRIVACY AND SECURITY
TERMS AND CONDITIONS

The following terms and conditions, as applicable to the services and/or goods provided to Tennessee Tech, shall govern the use of Personal Information by the parties. For purposes of this document, "Contractor" includes Contractor and any of its subcontractors.

I. Data Privacy:

a)
vidual including, without limitation, employee
s, passwords or PINs, financial account numbers,
urity questions and other personal identifiers.

Where applicable, "Personal Information" may also mean any information relating to an identified or identifiable natural person

a) 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.

b) 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.

2) 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

c) 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.

d) Cyber Insurance.

Contractor shall carry error & omissions and cyber liability insurance in an amount not less than $2,000,000 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 $2,000,000 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.