FLORIDA STATE UNIVERSITY

Information Privacy and Security

Standard Terms and Conditions

August 16, 2019

Version 1.42

The Information Security and Privacy standard Terms and Conditions contained herein are hereby incorporated in and attached to Agreements or Contracts by and between the Florida State University Board of Trustees (University) and **Contractor ("the Parties")** by reference. **Contractor** agrees to include all Terms and Conditions contained in this document in all subcontractor or agency contracts providing services under said Contract or Agreement. Capitalized terms in this document are defined in the current Florida State University policies.

I. OBSERVANCE OF LAWS AND REGULATIONS

The **Contractor,** when applicable, will ensure, the data types defined in the agreement designated for transfer or collection as part of agreed upon services will be provided to, or on behalf of, the University in a fully compliant manner to enable the University to meet relevant requirements of all laws, regulations, and contractual requirements applicable to the University, including, but not limited to, the current versions of:

Student Financial Aid Data

1) Gramm-Leach-Bliley Act (GLB) (15 U.S.C. §§ 6801(b) and 6805(b)(2));
2) Federal Trade Commission Red Flags Rule;

Student Record Data

3) Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g and 34 CFR Part 99);

Contractor agrees student education records are subject to the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g and 34 CFR Part 99 and the regulations promulgated thereunder. Such records are considered confidential and are therefore protected. To the extent that **Contractor** has access to education records protected under this contract, **Contractor** acknowledges it will be considered a "school official," as that term is used in FERPA at 34 C.F.R. § 99.31(a)(1)(i)(B), and (ii), and agrees it will comply with the requirements in FERPA concerning the confidentiality and release of education records. In compliance with FERPA, **Contractor** agrees that it shall not use education records for any purpose other than in the performance of this contract.

Personal Health Information

4) Health Insurance Portability and Accountability Act of 1996 (HIPAA) Pub. L. 104–191, 110 Stat. 1936a);
5) Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009;

Contractor agrees any transfer or collection of HIPAA and HITECH protected health information by or on behalf of a University Covered Component or Business Associate will be *governed under the provisions of a HIPAA Business Associates Agreement* between the University and the **Contractor**.

Credit Card Data

6) Payment Card Industry Data Security Standard (PCI DSS);

Contractor agrees to maintain a PCI DSS compliant environment if responsible for agreed upon credit card services for the University including the provisions of **Appendix B** in this document.

Research Data

7) International Traffic in Arms Regulations (ITAR);
8) Export Administration Regulations (EAR);
9) Controlled Unclassified Information in Nonfederal Systems and Organizations NIST Special Publication 800-171;

Email and Marketing Services

10) The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)

    Contractor agrees to meet CAN-SPAM Act provisions upon any agreed upon services involving email communication services to prospective students or marketing University events.

General Data Protection Regulation (In combination with Appendix A -Data Processing Agreement)

11) European General Data Protection Regulation (GDPR) (EU 2016/679) for select data collected or transferred from the European Economic Area;

    Contractor agrees any transfer or collection of GDPR protected personal information by or on behalf of the University will be governed under the provisions of the GDPR Data Processor Agreement **(Appendix A)** between the University and the **Contractor.**

Personal Information as Defined in Florida Statutes

12) Florida Information Protection Act, Florida Statute 501.171.

II. COMPLIANCE WITH FAIR INFORMATION PRACTICE PRINCIPLES

Contractor will post a notice of an entity's privacy practices prior to the collection of personally identifiable information on any public websites utilized as part of the contracted services. A privacy notice must:

1) Include a legitimate name and physical address of the entity collecting the data;
2) Identify the type of data collected;
3) Describe how the collected data will be used;
4) Describe any potential disclosure of personal information to third-parties, or, by third parties;
5) Describe any potential secondary use of personal information.

III. DISCLOSURE OF DATA

A. Except as otherwise expressly prohibited by law, **Contractor** will:

    1) Immediately notify the University of any subpoenas, warrants, or other legal orders, demands or requests received by **Contractor** seeking University Data;
    2) Consult with the University regarding its response;
    3) Cooperate with the University's reasonable requests in connection with efforts by the University to intervene and quash or modify the legal order, demand or request;
    4) Upon the University's request, provide the University with a copy of its response.

B. If the University receives a subpoena, warrant, public records request, or other legal order, demand or request seeking University Data maintained by **Contractor**, the University will promptly provide a copy to **Contractor**. **Contractor** will promptly supply the University with copies of data required for the University to respond and will cooperate with the University's reasonable requests in connection with its response.

IV. SAFEGUARD STANDARD

A. **Contractor** shall implement, maintain and use appropriate administrative, technical and physical security

measures to preserve the confidentiality (authorized access), integrity and availability of the Protected or Private Information. While **Contractor** has responsibility for the Protected or Private Information under the terms of its contract or agreement, **Contractor** shall ensure that such security measures are regularly reviewed and revised to address evolving threats and vulnerabilities.

B. **Contractor** shall not store, process, transmit, or provide remote support to University Protected or Private Information outside of data centers and support personnel located in the United States without the express prior written approval of the University.

C. **All facilities** used to store, process, or transmit Protected or Private Information will employ commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure **Contractor's** own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved.

D. **Contractor** warrants that all Protected or Private Information will be encrypted in transmission (including via web interface) and may require encrypted storage at no less than 128-bit level encryption as negotiated by the University.

E. **Contractor** will use industry standard and up-to-date security tools and technologies such as antivirus protections, antimalware and ransomware protections, and intrusion prevention and detection methods in providing Services under this Agreement.

F. **Contractor** will adhere to additional controls in Appendix B should it store, process, or transmit cardholder or sensitive authentication data associated with the contractual requirements of the Payment Card Industry-Data Security Standard (PCI DSS) published by the Payment Card Industry Security Standards Council.

V. DATA TRANSFER UPON TERMINATION OR EXPIRATION

A. Within 30 days of the termination, cancellation, expiration or other conclusion of the Agreement, **Contractor** shall return the Protected or Private University data to the University in an agreed upon format, unless the University requests in writing that such data be destroyed. This provision shall also apply to all Protected or Private Information that is in the possession of subcontractors or agents of **Contractor**. Such destruction shall be accomplished by "purging" or "physical destruction" in accordance with commercially reasonable standards for the type of data being destroyed (e.g., *Guidelines for Media Sanitization*, NIST Special Publication 800-88 Revision 1. **Contractor** shall certify in writing to University that such return or destruction has been completed. Notwithstanding the expiration or termination of these terms for any reason, the obligations of confidentiality and non-use set forth in this document shall extend for a period of five years after such expiration or termination.

B. **Contractor will notify the University of impending cessation of its business** and any contingency plans. This includes immediate transfer of any previously escrowed assets and data and providing the University access to **Contractor's** facilities to remove and destroy University-owned assets and data. **Contractor** shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the University. **Contractor** will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the University. **Contractor** will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and effect on the University, all such work to be coordinated and performed in advance of the formal, final transition date.

VI. BREACHES OF PROTECTED INFORMATION

A. **Definition**. For purposes of this article, the term, "Security or Privacy Breach," has the meaning given to it under the applicable Florida Statute (F.S. 501.171(1)(a)), applicable state or federal rule/regulation, or contractual obligation.

B. **Upon becoming aware of a Security or Privacy Breach**, or of circumstances that could have resulted in unauthorized access to or disclosure or use of University Data, **Contractor** will notify the University within 48-hours or as stipulated below for GLB/PCI DSS/NIST 800-171, fully investigate the incident, and cooperate fully with the University's investigation of and response to the incident. Except as otherwise required by law, **Contractor** will not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the University.

1) **Gramm-Leach-Bliley Act** (GLB) (15 U.S.C. §§ 6801(b) and 6805(b)(2)) (Select Student Aid Data)- **Contractor** must report any "suspected" data breach on the day it is detected;

2) **Payment Card Industry Data Security Standard** (PCI DSS) (Credit Card Data)- **Contractor** shall report both orally and in writing to the University. In no event shall the report be made more than one (1) day after **Contractor** knows or reasonably suspects a Breach has or may have occurred;

3) **Controlled Unclassified Information in Nonfederal Systems and Organizations NIST Special Publication 800-171** (Select Research Data)- **Contractor** shall report both orally and in writing to the University. The report should be made more within one (1) day after **Contractor** knows or reasonably suspects a breach has or may have occurred.

C. **Contractor's Security and Privacy Breach Report** shall identify:

1) The nature of the unauthorized access, use or disclosure;

2) The Protected or Private Information accessed, used or disclosed;

3) The person(s) or entities who accessed, used and disclosed and/or received Protected or Private Information (if known);

4) What **Contractor** has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure;

5) What corrective action **Contractor** has taken or will take to prevent future unauthorized access, use or disclosure;

6) **Contractor** shall provide such other information, including a written report, as reasonably requested by University.

D. **Costs Arising from Breach.** In the event of a Breach by the **Contractor** or subcontractor, **Contractor** agrees to indemnify and hold harmless the University arising from such Breach, including but not limited to costs of notification of individuals, establishing and operating call center(s), credit monitoring and/or identity restoration services, time of University personnel responding to Breach, civil or criminal penalties levied against the University, attorney's fees, court costs, etc. Any Breach may be grounds for immediate termination of this Agreement by the University.

VII. BUSINESS CONTINUITY AND DISASTER RECOVERY

Notwithstanding business continuity and disaster recovery terms established in **Contractor's** current University contract or agreement which: negate, modify, or supersede the requirements included in this section; University confirmation that **Contractor** business continuity and disaster recovery capabilities are not required; or, business continuity and disaster recovery capabilities that are required by law, **Contractor** is responsible for having a Business Continuity Plan.

In the event of a Public or Institutional Emergency, **Contractor** will implement the applicable actions set forth in its Business Continuity Plan and will make other commercially practicable efforts to mitigate the impact of the event on the University. For clarification of intent, being obliged to implement the Plan is not of itself an occurrence of force majeure, and **Contractor** will not be entitled to any additional compensation, extension of time, or other accommodation, by virtue of having to implement its plan, unless otherwise agreed to by the University in writing. A Public or Institutional Emergency means a natural or manmade event that creates a substantial risk to the public, that causes or threatens death or injury to the general public, or that causes a significant disruption to the day-to-day business operations of the University.

VIII. RIGHT TO AUDIT

Contractor agrees that, as required by applicable state and federal law, auditors from state, federal, Florida State University, or other agencies so designated by the State or University, shall have the option to a technology audit including obtaining the **Contractor's** latest public version of a SOC2 Type 2 report in addition to any financial audit terms of the outsourced service. Records pertaining to the service shall be made available to auditors and the University during normal working hours for this purpose.

Florida State University (Employee Authorized to Bind University)

Signature_____

Name:_____

Title:_____

Date Signed: _____

Contractor

Signature_____

Name_____

Title_____

Date Signed _____

Appendix A - GDPR Data Processor Agreement

WHEREAS

(A) The university acts as a Data Controller.

(B) The university wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "**Agreement**" means this Data Processing Agreement and all Schedules;

1.1.2 "**University Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of university pursuant to or in connection with the Principal Agreement;

1.1.3 "**Contracted Processor**" means a Subprocessor;

1.1.4 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 "**EEA**" means the European Economic Area;

1.1.6 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.8 "**Data Transfer**" means:

1.1.8.1 a transfer of university Personal Data from the university to a Contracted Processor; or

1.1.8.2 an onward transfer of university Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 "**Services**" means the agreed upon processing activities the **Contractor** provides as defined in the master agreement.

1.1.9 "**Subprocessor**" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the university in connection with theAgreement.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of university Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of university Personal Data;and

2.1.2 not Process university Personal Data other than on the relevant university's documentedinstructions.

2.2 The university instructs Processor to process university Personal Data.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the university Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant university Personal Data, as strictly necessary for the purposes of the Master Service Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the university Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Processor shall take account the risks that are presented by Processing, in particular from a Personal DataBreach.

5. Subprocessing

5.1 Processor shall not appoint (or disclose any university Personal Data to) any Subprocessor unless required or authorized by the university. All subprocessing must occur pursuant to contractual terms necessitating the protection of university data as required herein.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist the university by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the university obligations, as reasonably understood by university, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify university if it receives a request from a Data Subject under any Data Protection Law in respect of university Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of university or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform university of that legal requirement before the Contracted Processor responds tothe request.

7. Personal Data Breach

7.1 Processor shall notify university without undue delay upon Processor becoming aware of a Personal Data Breach affecting university Personal Data, providing university with sufficient information to allow the university to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the university and take reasonable commercial steps as are directed by university to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Processor shall provide reasonable assistance to the university with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which university reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of university Personal Data by, and taking into account the nature of the Processing and information available to, the ContractedProcessors.

9. Deletion or return of university Personal Data

9.1 Subject to this section 9 Processor shall promptly and in any event within 30 business days of the date of cessation of any Services involving the Processing of university

Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of those university Personal Data.

9.2 Processor shall provide written certification to university that it has fully complied with this section 9 within 30 business days of the Cessation Date.

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to the university on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the university or an auditor mandated by the university in relation to the Processing of the university Personal Data by the Contracted Processors.

10.2 Information and audit rights of the university only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the university. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. General Terms

12.1 **Confidentiality.** Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("**Confidential Information**") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain.

12.2 **Notices.** All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

Appendix B – Payment Card Industry Safeguard Standards

A. If **Contractor** is storing, processing, or transmitting cardholder data, or is accepting sensitive authentication data, as defined by the PCI DSS (Payment Card Industry Data Security Standard), **Contractor** agrees to maintain compliance with the current effective version of the PCI DSS throughout the term of the Agreement or Contract with the University. Upon request by the University, **Contractor** will provide a current PCI DSS Attestation of Compliance.

B. If **Contractor** is utilizing a Payment Card Industry Security Standards Council (PCI SSC) approved Point-to-Point Encryption (P2PE) solution to accept or process credit card payments, **Contractor** is responsible for the solution's proper implementation and operation in compliance with all applicable PCI DSS, P2PE, and PCI SSC requirements. **Contractor** responsibilities include ensuring that the P2PE solution maintains its PCI SSC approval status throughout the term of its agreement or contract with the University. Upon request by the University, **Contractor** will provide a current P2PE Instruction Manual, and P2PE Report on Validation (ROV) for the Solution, Application and Components being utilized.

C. If **Contractor** is utilizing a University-approved third-party vendor P2PE or End-to-End Encryption (E2EE) solution to accept or process credit card payments, **Contractor** is responsible for the solution's proper implementation and operation in compliance with all applicable PCI DSS, PCI SSC and third-party vendor solution requirements throughout the term of the Agreement or Contract with the University. **Contractor** also is responsible for providing a responsibility matrix identifying the PCI DSS controls that the University is responsible for meeting and the controls that will be met by contractor as required by the current version of the PCI DSS. Upon request by the University, **Contractor** will provide the results of any PCI DSS assessments used to support or develop the responsibility matrix relevant to the third-party P2PE or E2EE solution.

D. If **Contractor** is utilizing a payment application that is Payment Application Data Security Standard (PA-DSS) validated, **Contractor** is responsible for maintaining its PA-DSS compliance status throughout the term of the Agreement or Contract with the University. Upon request by the University, **Contractor** will provide a current PA-DSS Report on Validation certifying the PA-DSS compliance status of the payment application.