Third Party Technology Vendor
Security and Privacy
Terms and Conditions Agreement

October, 2024

I. COMPLIANCE WITH LAWS AND REGULATIONS

The Third Party Technology Vendor must ensure that data and systems defined in the agreement designated for transfer, processing, or collection as part of agreed upon services will be provided to, or on behalf of, Northern Kentucky University in a fully compliant manner to enable the University to meet relevant requirements of all laws, regulations, compliance and contractual requirements applicable to NKU. This includes, but is not limited to current versions of:

Student Financial Aid Data

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

Student Record Data

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

  Third Party Technology Vendor 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 the Third Party Technology Vendor has access to education records protected under this contract, Third Party Technology Vendor 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, Third Party Technology Vendor agrees that it shall not use education records for any purpose other than in the performance of this contract.

Personal Health Information

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

  Third Party Technology Vendor agrees any transfer or collection of HIPAA and HITECH protected health information by or on behalf of the University will be governed under the provisions of a HIPAA Business Associates Agreement between the University and the Third Party Technology Vendor

Research Data

- International Traffic in Arms Regulations (ITAR)
- Export Administration Regulations (EAR)

- Controlled Unclassified Information in Nonfederal Systems and Organizations NIST Special Publication 800-171

Email and Marketing Services

- The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)
- Third Party Technology Vendor agrees to meet CAN-SPAM Act provisions upon any agreed upon services involving email communication services to prospective students or marketing University events.
- Third Party Technology Vendor must not sell or make available any University information unless express permission is granted by the proper NKU authorities, and then only used for the designated purposes of the data.

General Data Protection Regulation

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

  Third Party Technology Vendor 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 Third Party Technology Vendor.

Payment Card Industry – Data Security Standards (PCI-DSS) for Credit and Payment Cards

- Third Party Technology Vendor agrees to maintain a PCI DSS standards compliant environment (according to the current, effective version of PCI DSS administered by the Payment Card Industry Security Standards Council) if responsible for agreed upon credit card services for the University including any and all provisions referenced in this document

- Third Party Technology Vendor will comply with any additional requirements as defined in the **NKU PCI-DSS Standard** 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.

- Third Party Technology Vendor agrees any transfer, storage, or processing of payment card, or card holder data information by or on behalf of the University will be governed under the provisions of the Payment Card Industry Safeguard Standards (***Appendix B***) between the University and the Third Party Technology Vendor.

Personal Information as Defined in Kentucky Statutes

- Kentucky Data Privacy Laws, KRS 61.931 to 61.934, KRS 365.732, KRS 365.734

II. COMPLIANCE WITH FAIR INFORMATION PRACTICE PRINCIPLES

Third Party Technology Vendor will post a notice of NKU'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:

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

III. DISCLOSURE OF DATA

A. Except as otherwise expressly prohibited by law, Third Party Technology Vendor will:
   - Immediately notify the University of any subpoenas, warrants, or other legal orders, demands or requests received by Third Party Technology Vendor seeking University Data;
   - Consult with the University regarding its response;
   - 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;
   - 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 the Third Party Technology Vendor, the University will promptly provide a copy of the subpoena to Third Party Technology Vendor. The Third Party Technology Vendor 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. PHYSICAL, TECHNICAL, AND ADMINISTRATIVE SECURITY AND PRIVACY REQUIREMENTS FOR DATA AND INFORMATION HANDLING

A. Third Party Technology Vendor must read and understand the definitions for data classifications can be found in the **NKU Information Security Policy** in order to apply necessary security controls, practices, and governance defined herein.

B. The Third Party Technology Vendor must use unique, approved, and secured credentials if/when accessing NKU systems or data. The Third Party Technology Vendor is not authorized to connect computers, or network devices to non-public NKU networks without appropriate IT approvals beforehand, and that if access is granted, it will be limited to the lowest level of access necessary for the service or support requirements. All Third Party Technology Vendor access should be considered granted as a temporary, need-to-know basis, as bound by the time of the effective contract or engagement. Access may be removed by NKU at any time, if/when necessary in order to protect the University's data or interests.

C. The Third Party Technology Vendor shall implement, maintain and use industry-based, appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of the Confidential or Private Information (including but not limited to using Digital Signatures, Code Signing, and herein, defined in the Northern Kentucky University Information Security policy data classification categories).

D. The Third Party Technology Vendor must not store, process, transmit, or provide remote support to University Confidential or Private data outside of datacenters and support personnel located in the United States without prior express written permission by an appropriate authorized representative of the University.

E. Third Party Technology Vendor employees must provide updated training and awareness activities to validate their roles and responsibilities in maintaining the technical safeguards on behalf of the University. Third Party Technology Vendor employees are prohibited from transmitting, processing, or storing local copies of University data in any form for non-business support reasons.

F. All non-NKU facilities used to store, process, or transmit Confidential 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 Third Party Technology Vendor'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.

G. Third Party Technology Vendor warrants that all Confidential or Private Information will be encrypted in transmission (including via web interface) with at least TLS 1.2 and may require encrypted storage at no less than 128-bit level encryption as approved by the University's Information Security department.

H. Third Party Technology Vendor 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.

I. While Third Party Technology Vendor has responsibility for the Confidential or Private Information under the terms of its contract or agreement, Third Party Technology Vendor shall ensure that such security controls, practices, and governance are regularly reviewed and revised to address evolving threats and vulnerabilities and protect the University's data and information. The Third Party Technology Vendor should provide verifiable evidence to the University of regular security assessments or audits (ex. SOC 2, type 2, SOC3, PIAs etc.)

to ensure security and privacy controls and standards are properly maintained. The University reserves the right to request such evidence at any time during the contract or engagement for any reason, or to conduct its own security assessment of the Third Party Technology Vendor.

V. DATA TRANSFER UPON TERMINATION OR EXPIRATION

A. Within 30 calendar days of the termination, cancellation, expiration or other conclusion of the Agreement, Third Party Technology Vendor shall return the Confidential 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 Confidential or Private Information that is in the possession of sub-Third Party Technology Vendors or agents of Third Party Technology Vendor. 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. Third Party Technology Vendor 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. Third Party Technology Vendor 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 Third Party Technology Vendor's facilities to remove and destroy University-owned assets and data. Third Party Technology Vendor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the University. Third Party Technology Vendor 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. Third Party Technology Vendor 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.

C. If the Third Party Technology Vendor does not return or provide written verification for the destruction of University data or information within 30 calendar days of the termination, cancellation, expiration or other conclusion of the Agreement without a prior written, agreed upon arrangement, the Third Party Technology Vendor may be held liable for breach of contract and other suitable damages, at the Third Party Technology Vendor's expense.

VI. RESPONDING TO SECURITY OR PRIVACY ISSUES

During the course of the relationship between NKU and a Third Party Technology Vendor, security incidents may arise that affect NKU user or system data or privacy. Except as otherwise expressly prohibited by law, when such events occurs, the Third Party Technology Vendor must notify Northern Kentucky University:

A. Within the timeframes for legally defined data breach notification, as prescribed by local, state, federal and or applicable international laws. In Kentucky, Rev. Stat. 365.732 requires notification of breach to the State Attorney General within 72 hours of being notified by the "non-affiliated third party" or

B. Within the shortest, reasonable timeframe that would not detrimentally impact an active investigation or case, but provide NKU with a timely, competent response to identify and take appropriate actions to protect and inform affected NKU parties.

    1) **Gramm-Leach-Bliley Act** (GLB) (15 U.S.C. §§ 6801(b) and 6805(b)(2)) (Select Student Aid Data)-Third Party Technology Vendor must report any "suspected" data breach on the day it is detected;
    2) **Payment Card Industry Data Security Standard** (PCI DSS) (Credit Card Data)- Third Party Technology Vendor shall report both orally and in writing to the University. In no event shall the report be made more than one (1) day after Third Party Technology Vendor 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)- Third Party Technology Vendor shall report both orally and in writing to the University. The report should be made more within one (1) day after Third Party Technology Vendor knows or reasonably suspects a breach has or may have occurred.

C. Third Party Technology Vendor's Security and Privacy Breach Report shall identify:

    1) The nature of the unauthorized access, use or disclosure;
    2) The Confidential or Private Information accessed, used or disclosed;
    3) The person(s) or entities who accessed, used and disclosed and/or received Confidential or Private Information (if known);
    4) What Third Party Technology Vendor has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure;
    5) What corrective action Third Party Technology Vendor has taken or will take to prevent future unauthorized access, use or disclosure;
    6) Third Party Technology Vendor 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 Third Party Technology Vendor or sub-Third Party Technology Vendor, Third Party Technology Vendor 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.

E. Any Breach or non-compliance to respond in a commercially reasonable and timely manner to security or privacy issues may be grounds for immediate termination without penalty to the University, of this Agreement and any contractual obligations the University has to the Third Party Technology Vendor.

VII. ARTIFICIAL INTELLIGENCE (AI) USAGE AND RESTRICTIONS

Third Party Technology Vendors must obtain formal permission in writing by the University when AI will be used when services are provided or subscribed to. This can be in the form of a contract, SOW, service agreement or other binding written instrument to which the University must read and agree. The documentation shall provide transparent and accurate details on AI usage by the Third Party Technology Vendors in service to the University.

Third Party Technology Vendors must comply with all applicable laws, regulations, and industry standards related to the development, use, and deployment of AI technologies to any University data, systems, or identities. This includes, but is not limited to, requirements regarding data privacy, security, bias mitigation, transparency, and responsible AI practices.

Third Party Technology Vendors shall not use AI in a manner that discriminates against or harms any individual or group based on protected characteristics such as race, ethnicity, gender, religion, age, disability, or sexual orientation.

Third Party Technology Vendors must ensure that AI systems are designed and used in a transparent and accountable manner, with appropriate safeguards to prevent unintended consequences and mitigate risks. Data stored by and usage of AI falls within the bounds of the University's Right to Audit / Review, Section X.

Third Party Technology Vendors shall maintain the confidentiality and security of any data used to train or operate AI systems, and shall implement appropriate measures to protect such data from unauthorized access, use, or disclosure in accordance with this Terms and Conditions document.

Third Party Technology Vendors shall regularly assess and monitor the performance and impact of AI systems to identify and address any potential biases, errors, or unintended consequences and report or otherwise disclose details or findings relevant to the University.

Third Party Technology Vendors must provide ongoing, timely, and accurate information to the University regarding the use of AI in the performance of Services, including the specific AI technologies employed, their limitations, and the potential impact on the Services.

Third Party Technology Vendors shall cooperate with the University in any investigation or dispute related to the use of AI in the performance of Services.

Data created by Third Party Technology Vendors AI usage for University data, systems, and identities falls under the governance of section **V: DATA TRANSFER UPON TERMINATION OR EXPIRATION**

VIII. PROVIDE ISSUE MITIGATION AND REMEDIATION

The IT service provider is responsible to address and solve operational, security, or privacy issues that affect NKU users and/or systems within a timeframe that returns the information, data, or services to the contractual state of security, operation, or performance level within one (1) hour, or as soon as commercially reasonable, at no additional cost to NKU.

IX. PROVIDE DISASTER RECOVERY AND BUSINESS CONTINUITY

Third Party Technology Vendors must provide attestable evidence that disaster recovery plans addressing technical operations and business continuity plans that address business process resiliency are in place. Plan testing should occur at regular intervals and attestations provided to NKU within six (6) months which summarizes the test outcomes.

X. RIGHT TO AUDIT / REVIEW

The Third Party Technology Vendor agrees that, upon request, applicable governing agencies so designated by the State or the University shall have the option to a technology audit including obtaining the Third Party Technology Vendor's latest public SOC 2, Type 2 or SOC 3 report and related documents such as bridge letters or relevant financial audit terms. NKU may require that the Third Party Technology Vendor provide additional verification of security or privacy testing and controls based on the risk to NKU.

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 Terms and Conditions Agreement shall have the following meaning:

1.1.1. **"Agreement"** means this Terms and Conditions Agreement document, the NKU Technology Vendor and Third Party Management Policy, and any relevant NKU policies;

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 NKU Personal Data from the university to a Contracted Processor; or

1.1.8.2. an onward transfer of NKU 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 Third Party Technology Vendor provides as defined in the master agreement.

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

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 documented instructions.

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 Third Party Technology Vendor 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. Considering 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 Data Breach.

5. Subprocessing

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

6. Data Subject Rights

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

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 to the request.

7. **Data Protection Impact Assessment and Prior Consultation**

7.1. 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 Contracted Processors.

8. Deletion or return of University Personal Data

8.1. Subject to 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.

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

9. Audit Rights

9.1. Subject to 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.

9.2. 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.

10. Data Transfer

10.1. 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.

11. General Terms

11.1. **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.

11.2. **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 Third Party Technology Vendor 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), Third Party Technology Vendor 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, Third Party Technology Vendor will provide a current PCI DSS Attestation of Compliance.

B. If Third Party Technology Vendor 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, Third Party Technology Vendor is responsible for the solution's proper implementation and operation in compliance with all applicable PCI DSS, P2PE, and PCI SSC requirements. Third Party Technology Vendor 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, Third Party Technology Vendor will provide a current P2PE Instruction Manual, and P2PE Report on Validation (ROV) for the Solution, Application and Components being utilized.

C. If Third Party Technology Vendor is utilizing a University-approved third-party vendor P2PE or End-to-End Encryption (E2EE) solution to accept or process credit card payments, Third Party Technology Vendor 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. Third Party

Technology Vendor 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 Third Party Technology Vendor as required by the current version of the PCI DSS. Upon request by the University, Third Party Technology Vendor 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 Third Party Technology Vendor is utilizing a payment application that is Payment Application Data Security Standard (PA-DSS) validated, Third Party Technology Vendor 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, Third Party Technology Vendor will provide a current PA-DSS Report on Validation certifying the PA-DSS compliance status of the payment application.

E. If Third Party Technology Vendor fails to comply with PCI-DSS and PA-DSS (whenever applicable), the Third Party Technology Vendor will take immediate, timely and appropriate actions to return the University's operation to an appropriate state of compliance. If the Third Party Technology Vendor is the responsible party for becoming non-compliant, then any and all costs associated with penalties, and remediation actions incurred by non-compliance will be borne solely by the Third Party Technology Vendor.

Signatures below indicate acknowledgement, understanding and agreement to abide by the Terms and Conditions set forth in this document, to be upheld the duration of the contract or engagement.

_____	_____
Third Party Technology Vendor, **Account Executive or Authorized Representative**	**Date**
_____	_____
Northern Kentucky University **CISO, CIO or Authorized Representative**	**Date**