Northern Michigan University

VENDOR PRIVACY AGREEMENT

This Vendor Privacy Agreement ("Agreement") is incorporated into, amends and supersedes the contract for services ("Contract") between Northern Michigan University ("NMU") and Vendor. If Vendor or Vendor's system stores, processes or transmits "confidential data" (as defined in NMU's Policies, described further below), then as a condition of doing business, or continuing to do business, with NMU and in consideration for payments under the Contract and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, Vendor agrees to be bound by the following terms and conditions:

1. **Compliance**. Vendor acknowledges that NMU has adopted an Acceptable Use Policy, a Vendor Privacy Policy, and a Data Classification Policy, copies of which are set forth in Attachment A (collectively, "Policies"). Vendor agrees to abide by NMU's Policies, as may be amended from time to time, and to cause its employees, agents and subcontractors to abide by the Policies, in connection with the Contract and their provision of services thereunder. In the event of a conflict between the terms of this Agreement and any provision in any of the Policies, the terms of this Agreement shall prevail. Additionally, Vendor shall comply with all applicable Michigan and federal laws, including those regarding access to and protection of personal and electronic data. Vendor specifically acknowledges its responsibility to understand and comply with all privacy laws as may be applicable to the Contract, including but not limited to the Gramm-Leach-Bliley Act, the Family Educational Rights and Privacy Act and the Health Insurance Portability and Accountability Act.

2. **Confidential Information**. Vendor agrees that business and other proprietary information of any type, which is generated in connection with work related to NMU's operations and is not generally known to the public, is confidential. Such information may include student education records, treatment records, personnel information, business deliberations, compliance-related information, notes, minutes, documents, network transmissions or electronically or magnetically stored data/records, including IT Data, as defined further below (collectively, "Confidential Information"). Such information shall not be accessed, directly or indirectly disclosed, used, copied, distributed or republished for any reason other than to perform services under the Contract. Vendor shall not allow any third party to have access to any Confidential Information unless otherwise approved by NMU in writing. Confidential Information learned or created during the course of Vendor's relationship with NMU shall not be used or disclosed by Vendor after termination of the relationship. Confidential Information does not include information that: (a) is readily available to the public, but not due to a data breach, or fault of Vendor; (b) was independently obtained by Vendor from a third party who is lawfully in possession of such information and not bound by a non-disclosure obligation with respect to such information; or (c) was already in Vendor's possession for reasons unrelated to the Contract or an existing agreement with NMU.

3. **Access to Information and IT Assets**. Vendor acknowledges and agrees that NMU's computers, applications, information storage, networks and telecommunications systems, ("IT Assets") are NMU's property. The IT Assets will be used only by properly identified, authenticated and authorized individuals and shall be used solely for NMU's business. NMU retains all ownership, title, rights and control over all messages, content, data, information and files composed, stored, sent or received on IT Assets ("IT Data"). Vendor shall not access Confidential Information or NMU data, files or any other stored information not necessary for Vendor's performance under the Contract. Vendor acknowledges and agrees that Vendor has no expectation of privacy with respect to use of the IT Assets.

4. **Vendor Employees, Agents and Subcontractors**. Vendor shall require its employees, agents and subcontractors to observe and comply with this Agreement. To the extent necessary, Vendor shall provide training to such employees, agents and subcontractors to promote compliance with this Agreement. Vendor agrees that NMU has the right to request and review the most current, annual third party audit report.

5. **Safeguard Standard**. Vendor agrees to use reasonable care to protect the privacy and security of Confidential Information by commercially acceptable standards and no less rigorously than it protects its own confidential information. Vendor shall implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of the Confidential Information. If Vendor stores Confidential Information on portable devices or media, such devices or media must be encrypted in accordance with the Federal Information Processing Standards (FIPS) Publication 140-2, as may be amended or superseded. Vendor shall ensure that security measures are regularly reviewed and revised to address evolving threats and vulnerabilities while Vendor has responsibility for the Confidential Information under the terms of this Agreement.

6. **Reporting Instances of Noncompliance**. Vendor agrees to report immediately any violations of the requirements of this Agreement, violations of the Policies or breaches (or potential breaches) of network security to NMU's Internal Auditor, by email auditor@nmu.edu AND phone (906) 227-2375.

7. **Data Breach Response**. If the nature of Vendor's business involves Vendor's equipment, software, products, hosts, networks or environments that may expose NMU IT Data or Confidential Information to a potential data breach, then Vendor shall have in place at all times a commercially reasonable incident response plan, which shall be made available to NMU for review upon request. If Vendor has any reason to believe that a data breach may have occurred on any of Vendor's equipment, software, products, hosts, networks or environments, Vendor shall immediately provide notice to NMU of all pertinent details related to the same while also taking such immediate actions as may be necessary to preserve relevant evidence, identify the nature of the event and contain any data breach. If it appears to NMU, in its sole discretion, that services or technology provided by Vendor are a source of the data breach and present an unreasonable risk, then, in addition to any other remedies, NMU may opt to discontinue use of that source of the data breach and NMU's corresponding payment obligations under the Contract shall be adjusted equitably. NMU shall have full control over determining notification requirements in the event of a potential or actual data breach affecting any of its Confidential Information or IT Data.

8. **Termination of Access and Procedures**. Vendor's access to NMU IT Assets and IT Data is subject to Vendor's continuing compliance with this Agreement, and NMU may suspend or revoke such access at any time and for any reason. Within 30 days of the termination, cancellation, expiration or other conclusion of the Contract or this Agreement, or if otherwise requested by NMU, Vendor shall return the IT Data to NMU, unless NMU requests in writing that such data be destroyed. Such destruction will be accomplished by "purging" or "physical destruction," in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88, as may be amended or superseded. Vendor shall certify in writing to NMU that such return or destruction has been completed.

9. **Notice and Approval of Offshoring**. Vendor represents and warrants to NMU that Vendor shall not, without NMU's prior written consent: (a) perform any of its obligations under this Agreement or the Contract from locations or using employees, contractors and/or agents, situated outside the United States; (b) directly or indirectly (including through the use of subcontractors) transmit or store any IT Data outside the United States; or (c) allow any IT Data to be accessed by Vendor employees, contractors and/or agents from locations outside the United States.

10. **Indemnity**. Vendor shall indemnify, hold harmless and defend NMU from and against any and all claims, losses, liabilities, costs and other expenses incurred as a result of, or arising directly or indirectly out of or in connection with, any unauthorized use of or access to the Confidential Information or any data or security breach that results from the acts or omissions of Vendor; except to the extent caused by NMU's negligence or misconduct.

11. **Additional Insurance**. Unless otherwise agreed in writing by NMU, Vendor at its sole cost and expense shall obtain and maintain insurance coverage for internet professional liability, cyber liability and social engineering liability, include coverage for privacy and data security breaches and reasonable costs in

investigating and responding to the breaches. Each policy shall provide minimum coverage of at least $2 million per occurrence and shall name Northern Michigan University as an additional insured, with proof of coverage provided to NMU upon request.

12. **Governing Law; Jurisdiction**. This Agreement shall be governed by Michigan law, without regard to conflicts of laws principles. Vendor consents to the exclusive jurisdiction of the Michigan Court of Claims and the state and federal courts in Marquette County, Michigan with respect to any matters arising under this Agreement.

13. **Remedies**. Vendor agrees that money damages would not be a sufficient remedy for any breach or potential breach of this Agreement by Vendor and that without limiting any other rights and in addition to all other remedies, NMU shall be entitled to seek specific performance and injunctive or other equitable relief without proof of damages and without the necessity of posting any bond or other security as a remedy for any such breach or potential breach. In the event NMU institutes any legal suit, action or proceeding against Vendor arising out of or relating to this Agreement, NMU shall be entitled to receive in addition to all other damages to which it may be entitled, the costs incurred by NMU in conducting the suit, action or proceeding, including reasonable attorneys' fees and expenses and court costs.

14. **Miscellaneous**. This Agreement may not be amended except by a writing signed by the parties. If any provision of this Agreement is held to be invalid, illegal or otherwise unenforceable, the holding shall not affect the remaining provisions. The waiver of any breach of this Agreement by either party hereto shall not constitute a continuing waiver or a waiver of any subsequent breach of either the same or any other provision. The covenants and obligations set forth in this Agreement that are intended to continue in effect after termination of any agreement with NMU shall survive termination and shall remain in effect and enforceable by NMU.

Vendor:

Company Name: _____

Address: _____ By: _____

_____ Print Name: _____

_____ Title: _____

_____ Date: _____

Northern Michigan University:

By: _____

Print Name: _____

Title: _____

Date: _____

Attachment A

NMU Acceptable Use Policy

Date approved: 12/16/19
Approved by: President
Oversight Unit: Information Technology and Technical Services
Level: Admin Policy

PURPOSE: The intent of this policy is to make clear certain uses which are and are not appropriate, not to exhaustively enumerate all such possible uses. This statement represents a guide to the acceptable use of network and computing resources which includes an array of institutional electronic business systems, computing services, networks, databases and other resources ("NMU IT resources"). Using these guidelines, Northern Michigan University ("NMU") may at any time make determinations that particular uses are or are not appropriate.

APPLICABILITY: Northern Michigan University students, faculty and staff and any user or provider of NMU IT resources, including any individual who uses, logs in, attempts to use or attempts to log in to a NMU system, whether by direct connection or across one or more networks, or who attempts to connect to or traverse a network, whether via hardware, software or both (each a "User").

POLICY: Central to appropriate and responsible use is the stipulation that network and computing resources shall be used in a manner consistent with the instructional, public service, research and administrative objectives of the University

RESPONSIBILITY: Users are responsible for informing themselves of any university policies, regulations or other documents that govern the use of NMU IT resources prior to initiating the use of NMU IT resources.

Privacy

- Users must respect the privacy of others. NMU Users who invade the privacy of others may have their access suspended and may also be subject to university disciplinary action. NMU will make reasonable efforts to maintain the confidentiality of files stored on university hardware and to safeguard the contents from loss, but is not liable for the inadvertent or unavoidable loss or disclosure of the contents, or for disclosure resulting from the unlawful acts of others. NMU has the right of access to investigate complaints and manage the network and computing resources of the University, and to keep records and files to the extent appropriate to administer those computing resources.
- While every effort is made to ensure the privacy of NMU Users, this may not always be possible. In addition, since employees are granted use of NMU IT resources to conduct University business, there may be instances when NMU, based on approval from authorized officers, reserves and retains the right to access and inspect stored information without the consent of the User.
- For your own personal protection and the protection of the University computing system, Users are expected not to share their User ID and password with any other persons.
- Users may not assume another person's identity or role through deception or without proper authorization. You may not communicate or act under the guise, name, identification, email address, signature or indicia of another person without proper authorization, nor may you communicate under the rubric of an organization, entity or unit that you do not have the authority to represent. Users shall not intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other Users, whether on the NMU campus or elsewhere, or develop or retain programs for that purpose.

System Integrity

- Users must respect the integrity of NMU's IT resources on campus and at all sites reachable by NMU's external network connections. Computing services and wiring may not be modified or extended beyond the area of intended use. This applies to all network wiring, hardware and in-room jacks. IT resources may not be used to provide unauthorized Internet access to anyone outside of the university for any purpose. Users shall not intentionally develop or use programs that harass other Users, that obstruct or disrupt use (or that could reasonably be expected to disrupt), or that attempt to damage, alter, or infiltrate (e.g. gain access without proper authorization) a computer, system or network, regardless of whether the resource used is securely protected against unauthorized use.
- To respect the shared nature of NMU IT resources, Users shall avoid activities that unreasonably tax system resources or that, through frivolous use, goes beyond the intended use of the system. This includes, for example, intentionally placing a program in an endless loop, printing excessive amounts of paper, or sending "spam," "chain letters" or other unsolicited mass mailings to lists or individuals and other types of use which would cause network congestion or otherwise interfere with the work of others.
- NMU IT resources may not be used to fundraise, advertise or solicit unless that use is approved in advance in writing by NMU. Furthermore, Users must not use NMU IT resources for partisan political purposes, such as using electronic mail to circulate advertising for political candidates.

Personal Information

- Users should be cautious about making information about themselves and others available on the Internet. NMU cannot protect Users from invasions of privacy, identity theft and other possible dangers that could result from the individual's distribution of personal information.

Use of Resources Accessed through NMU IT Resources

- When using NMU IT resources or resources owned by third parties that are accessed using NMU IT resources, Users must comply with all applicable federal and state laws, all applicable University rules, ordinances, and policies and the terms of any contract or license which governs the use of the third-party resource and by which the User or NMU is bound. Users must not use NMU IT resources to violate copyright, patent, trademark or other intellectual property rights.

User Compliance

- When using NMU IT resources and accepting any NMU issued computing accounts, Users agree to comply with this and all other computing related policies. Users have the responsibility to keep up-to-date on changes in the computing environment, as published, using NMU electronic and print publication mechanisms and to adapt to those changes as necessary.

United States Copyright Law

- Copyright is a form of protection provided by the laws of the United States (Title 17, U.S. Code) to the authors of "original works of authorship," including text and content, images, computer software, motion pictures, music and other media in both personal use and in production of electronic information. Unauthorized copying or downloading of copyrighted material is in violation of U.S. copyright laws. Users may not make or use illegal copies of copyrighted materials or software, store such copies on NMU IT resources or transmit them over NMU networks. Further, you may not attempt to override copy protection on commercial software. For more information on copyright and fair use provisions, go to the NMU Olson Library web site (http://www.nmu.edu/olsonlibrary).

The Law of the State of Michigan

- Act 53 of the Public Acts of 1979 of the State of Michigan is "An act to prohibit access to computers, computer systems, and computer networks for certain fraudulent purposes; to prohibit intentional and unauthorized access, alteration, damage, and destruction of computers, computer systems,

computer networks, computer software programs, and data; and to prescribe penalties." The penalties for violating this act follow: A person, who violates this act, if the violation involves $100.00 or less, is guilty of a misdemeanor. If the violation involves more than $100.00, the person is guilty of a felony, punishable by imprisonment for not more than ten (10) years, or a fine of not more than $5,000.oo or both.

Student Code

- Student behavior on and off campus is governed under the Student Code. All regulations related to communication and use of University resources also relate to Internet usage. Some examples include but are not limited to Harassment, or Unauthorized access to Information (http://www.nmu.edu/studenthandbook). Other University Student Code Regulations and Policies are listed in the NMU Handbook and can be accessed at http://www.nmu.edu/studenthandbook. All of the policies and regulations which are listed there also cover the use of computers and the Internet.

Disciplinary Actions Taken

- When NMU has reasonable cause to believe there has been inappropriate use, NMU staff may take immediate remedial action. In an emergency, to prevent further inappropriate activity, NMU computing staff may temporarily disconnect a User from the network or other NMU IT resources. Punishment for violation of the NMU Acceptable Use Policy may include, but is not limited to, temporary or permanent disconnection from NMU IT resources, suspension of a specific User's NMU ID for up to one (1) academic semester or further disciplinary action deemed necessary by the Dean of Students Office or where appropriate, the Human Resources Office, Office of the Provost and Vice-President for Academic Affairs or law enforcement agencies.

Information Disclaimer

- Individuals using NMU IT resources do so subject to applicable laws and NMU policies. NMU disclaims any responsibility and/or warranties for information and materials residing on or within NMU IT resources, non-NMU systems or publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of the State of Michigan, NMU, its faculty, staff or students.

Vendor Privacy Policy

Date approved: 12/16/19
Approved by: President
Oversight unit: Information Technology and Technical Services
Level: Admin Policy

This policy has a related procedure. Click to view procedure below.
This policy has a related guideline. Click to view guideline below.

Purpose:
This policy protects university data when it is entrusted to a third party.

Applicability:
All university personnel who contract with vendors who store, process or transmit university data defined as 'confidential' by the university's Data Classification Policy.

Policy:
As a condition of doing business or continuing to do business with NMU, vendors that store, process or transmit confidential data, must agree to the data protection criteria as provided in the university's Vendor Privacy Agreement. Exceptions to this policy may only be granted by the University's Committee on Information Security Operations.

Data Classification Policy

Date approved: 12/16/19
Approved by: President
Oversight unit: Information Technology and Technical Services
Level: Admin Policy

Purpose:
This policy provides standards to protect the confidentiality, integrity, and availability of university data. The policy applies regardless of the media on which the data resides.

Applicability:
All users of NMU Network Resources, administrative data, systems that access university data and media that store university data.

Policy:
Data will be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. Data security measures will be implemented commensurate with the value, sensitivity, and risk involved. Data will be protected and secured according to applicable federal and state requirements as well as university policies.

To implement security at the appropriate level, to establish guidelines for legal/regulatory compliance, and to reduce or eliminate conflicting standards and controls, data will be classified into one of the following categories:

Confidential: data that, if disclosed to unauthorized persons, would be a violation of federal or state laws and regulations, university policy, or university contracts. Any file or data that contains personally identifiable information of a trustee, officer, agent, faculty, staff, retiree, student, graduate, donor, or vendor may also qualify as confidential data. Confidential data includes but is not limited to:

- Medical records of any kind.
- Education records as defined by NMU's FERPA policy, except NMU IN numbers, which are classified as private.
- Unredacted unique government identifiers such as social security numbers.
- Research data, such as information supporting pending patents, grant applications, or information related to human subjects.
- Information access security, such as login passwords, personal identification numbers regulated by laws or regulations, digitized signatures, and encryption keys.
- Certain personnel records such as benefits records, health insurance information, retirement documents and/or payroll records.
- Library records as defined by the Michigan Library Privacy Act.
- Regulated primary account numbers, cardholder data, credit card numbers, banking information, or other information protected by consumer protection regulations and the payment card industry data security standards.
- Personal information protected from disclosure by state and federal identity theft laws including the Michigan Identity Theft Protection Act.
- Any data identified by state or federal law or government regulation, or by order of a court of competent jurisdiction to be treated as confidential or sealed by order of a court of competent jurisdiction.

Private: data that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be any law or other regulation requiring this protection. Private data is information that is managed and secured by personnel designated by the university who have a legitimate business purpose for accessing such data. Private data includes but is not limited to:

- Employment data.
- NMU Identification Numbers and redacted portions of government issued identification numbers.
- Business partner information where no restrictive confidentiality agreement exists.
- Planning documents.
- Alumni data.

Public: data to which the general public may be granted access in accordance with Northern Michigan University policy. Public data includes but is not limited to:

- Publicly posted press releases.
- Publicly posted schedules of classes.
- Posted university maps, newsletters, newspapers, and magazines.
- Directory information within the boundaries of NMU's FERPA Policy.
- Information posted on the university's public website including the website for Institutional Research.

Data owners, in conjunction with the Chief Technology Officer, the Assistant VP Information Services, and as appropriate, the Dean of Library and Instructional Support, or qualified designates, will develop, implement, and/or contract for appropriate data security using technology protocols, data encryption, data access controls, data retention and disposal procedures, data storage management, and end user training and awareness programs.

The Chief Technology Officer or a designate will regularly review this policy and the implementing procedures to ensure timely updates after legal, regulatory, technological, or other relevant changes.