Access and Data Sharing Agreement Between
the University of West Georgia
and _____

This data sharing agreement ("Agreement") is made and entered into this ___ day of ____ by the University of West Georgia ("UWG") and _____ ("Company").

RECITALS

WHEREAS, UWG has entered into a separate agreement with Company; and

WHEREAS, in order to provide the _____, Company will require access to UWG's network via (a remote connection, physical access, or both);

WHEREAS, in order to provide the_____, Company will require access to UWG's data;

NOW THEREFORE, in consideration of the mutual covenants and promises contained herein, the parties agree as follows:

AGREEMENT

1. **Purpose.** The Parties agree that Company will require access to (and, if applicable, store) UWG data in order to provide the Services detailed in the _____. This Access and Data Sharing Agreement outlines the specific responsibilities of the Company and UWG as it relates to the Company's access to any UWG data that may be stored within the Software or on the Server accessed or managed by the Company.
2. **Technical Services Point of Contact.** The Parties shall identify respective representatives on technical issues related to the implementation of the Services. The specific Points of Contact shall be listed in Appendix A of this agreement.
3. **Term of Agreement.** This Agreement supports and references the _____ entered into between the Parties and dated _____. The term of this Agreement runs with and concurrent to, and shall terminate in accordance with, the _____. Collectively the _____ and this Agreement shall be referred to as "Agreements."
4. **Grant of Access.** During the term of this agreement UWG agrees to grant Company access to the UWG Data necessary to support the business needs of the Software. The Company certifies that all systems and networking equipment that support, interact, or store UWG Data meet physical, network and system security requirements as defined by UWG in Section 6 of this Agreement or the standards identified by the National Institute of Standards of Technology (NIST) where UWG's requirements control in the event of conflict. Significant deviation from Section 6 of this agreement of NIST standards must be approved by the Information Security Officer within the Office of the Chief Information Officer. The Company will notify UWG within one (1) week if its systems and networking equipment do not conform to these requirements.

5. **Confidential Information.** The _____ provides that each Party shall treat the other Party's Confidential Information as confidential, and will not use or share said Confidential Information except as expressly set forth in the _____ or otherwise as authorized in writing by the Parties, or as may be required by applicable law. Additional uses of the data shared pursuant to this agreement may require an additional Access and Data Sharing Agreement. Confidential data also includes any user identifiable data collected in logs, cookies, or by other means.
    a. **UWG Confidential Information.** UWG is subject to several state and federal laws that define a privacy interest in records generated and kept by UWG. In addition, UWG is subject to established policies of the University System of Georgia. Company shall presume that all information that may be accessible or shared with Company during the term of this Agreement in relation to the Services to be provided pursuant to this Agreement is UWG Confidential Information unless otherwise designated by UWG.
    b. **Safeguarding Confidential Information.** The Company's employees, agents and subcontractors may have access to UWG Data to the extent necessary to carry out the Company's responsibilities under the agreement. The Company shall provide to UWG a written description of the Company's policies and procedures to safeguard confidential information, including evidence of adequate supervision and training to its agents, employees and subcontractors to ensure that UWG Data is not inadvertently disclosed.
    c. **Protected Student Data.** In the event that protected student data is shared with Company, UWG agrees to share student data elements with Company in a manner that safeguards the confidentiality of student data as defined by the Federal Family Educational Rights and Privacy Act (FERPA) and other applicable laws and regulations.
    d. **No Dissemination of Confidential Data.** No user identifiable and/or confidential data collected, maintained, or used in the course of performance of the Agreements shall be disseminated or published except as authorized by law and with written consent of UWG. Any UWG Data supplied to the Company shall be considered the property of the University System of Georgia and UWG. The Company must return any and all data collected, maintained, created or used in the course of the performance of the Contract, in whatever form it is maintained, promptly at the request of UWG.
    e. **Subpoena.** In the event that a subpoena or other legal process is served upon the Company for records containing confidential information, the Company shall promptly notify UWG and cooperate with the State in any lawful effort to protect the confidential information.
    f. **Reporting of Unauthorized Disclosure.** The Company shall within 24 hours of discovery report any unauthorized disclosure of UWG confidential information to the telephone number for the UWG contact listed on Appendix A.
    g. **Survives Termination.** The Company's confidentiality obligation under the Agreements shall survive termination of the Agreements.
    h. **Data Compromise.** Notwithstanding any other provision of this agreement, and in addition to any other remedies available to UWG under law or equity, Company agrees to reimburse UWG in full for all costs uncured by UWG to

remediate a Data Compromise that results from the negligence or misconduct on the part of Company, including but not limited to providing notification to third parties whose data were compromised and to regulatory agencies or other entities as required by law or contract; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Data Compromise.

6. **UWG Policies on Data Security.** The Company certifies that all systems and networking equipment that support, interact, or store UWG Data comply with the spirit and scope of the policies and standards found in UWG's Information Technology Security Plan, and meet the following requirements:
    a. **Equipment Protection.** Equipment shall be protected from theft, physical damage, electrical damage (power surges, etc.), water damage, fire damage, and logical damage (e.g. malware, viruses, etc.)
    b. **Principle of Least Access.** Institute a principle of least required access to perform a function.
    c. **Limit Root or Administrator Usage.** Avoid using root or administrator level accounts when a non-privileged account will satisfy the needs.
    d. **Privileged Access via Secure Encrypted Channel.** If a methodology for secure encrypted channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or web based SSL interface).
    e. **Security Patches.** Security patches shall be applied in a timely manner. If there is justifiable reason to not apply a security patch, then steps should be taken to mitigate any risk associated with not applying the patch. The justification and mitigation must be documented.
    f. **Data Storage Location.** All University data must be processed, stored, transmitted and disposed of onshore within the jurisdiction of the United States.
    g. **Audit Reports.** For hosted applications and services, Company will supply a current external audit report showing compliance with agreed upon standards.
    h. **Data Destruction.** At the completion of this agreement, Company will physically or electronically destroy beyond all ability to recover all customer data provided to them or collected as a part of the service or provided to Company's employees, subcontractors, agents, or other affiliated persons or entities. This includes any and all copies of the data such as backup copies created at any hosting site, metadata, and logging data that may have been collected during the service agreement. An extension may be granted by written agreement of the parties.
    i. **Data Return.** Upon request of UWG made before or within sixty (60) days after the effective date of termination, Company will make available to Customer for a complete and secure (i.e. encrypted and appropriated authenticated) download file of all Customer Data in an agreed upon format.
7. **Proprietary Rights.** You agree that no ownership rights of UWG Data are transferred to you under this Agreement. Further, Company shall not jeopardize the proprietary nature of any shared data by releasing, publishing, copyrighting, or otherwise publicly disseminating the data.
8. **Method of Access.** UWG provides various methods of access to computing and networking resources. Third party Company access is assessed and assigned on a case-

by-case basis. The Company and UWG must agree on a method of access that meets the business needs of UWG and the Company while mitigating the risks involved in conducting business over a public network.

a. **Agreed Upon Method.**
b. **Changes and Restrictions to Access.** UWG reserves the right to change or restrict the method of access to UWG Data at any time. UWG will notify the Company of intent to change the method of access no later than five (5) business days prior to the method change.
c. **System Degradation or Emergency.** In the event of significant degradation of system performance or other emergency, UWG may, in its sole discretion, temporarily suspend access under this Agreement in order to minimize threats to the operational stability and security of the UWG computing and networking environment.

9. **List of Known Incompatibilities.** Company agrees to identify and inform UWG in writing of any and all software that is known by Company to conflict with or cause issues with Company's software, including updates and patches for operating systems. This list shall be updated as necessary and communicated with UWG's Technical Point of Contact as soon as possible once the list update has been completed.
10. **Accessibility.** Company will supply a current Voluntary Product Accessibility template (VPAT Form) for any supplied software.
11. **Service Level Agreement.** Company will supply a current copy of the Service Level Agreement with response, resolution, and escalation times.
12. **Termination.** This Agreement shall take effect upon completion of signatures and remain in effect for one year or until terminated. This Agreement may be terminated by either UWG or Company upon notice to the other party. UWG may terminate this Agreement with or without cause at any time by providing written notice to Company thirty (30) calendar days prior to the termination date.
13. **Severability.** In the event of invalidity of any provision of this Agreement, the parties agree that such invalidity shall not affect the validity of the remaining provision of this Agreement.
14. **Governing Law.** This Agreement shall be governed and construed in accordance with the laws of the State of Georgia.

IN WITNESS THEREOF, the Parties have agreed to these terms and conditions as set forth above.

[Company Name]	Board of Regents, University System of Georgia / University of West Georgia
By: _____	By: _____
Date: _____	Date: _____
Name: _____	Name: _____
Title: _____	Title: _____

APPENDIX A

Company:

Name:
Title:
Street Address:
City, State:
Telephone Number:
Fax Number:
E-Mail Address:

Specify the Internet host machine(s), IP Address(es), and Ports which will be used to access the Network and/or Server (maximum of three systems). Additional hosts will require written approval by UWG ITS.

Host Name:	IP Address:	Port(s):

UWG:

Name:
Title:
Street Address:
City, State:
Telephone Number:
Fax Number:
E-Mail Address: