Confidentiality and Data Usage Agreement

This agreement (Agreement) is made between the Governor's Office of Student Achievement (GOSA), which houses the Georgia's Academic and Workforce Analysis and Research Data System (GA•AWARDS), and_____, recipient of private or protected data provided by GA•AWARDS, hereafter known as "Requestor." GOSA is entering into this Agreement on behalf of the GA•AWARDS Data Management Committee (DMC), which governs GA•AWARDS. The private and protected data about students, educators, workers, employers, or individuals, hereinafter referred to as "Subject Data," is collected to support the study or research on commercial, scientific, technical, or scholarly issues that has not been publicly released and contains de-identified, student-level information, the disclosure of which would jeopardize the receipt of federal funds under 20 U.S.C. § 1232g or its implementing regulations. As a result, the release and use of Subject Data is subject to the terms and conditions of this Agreement and is not subject to public review under O.C.G.A. § 50-18-70 and is expressly exempt from public review pursuant to O.C.G.A. § 50-18-72(a)(35)-(37).

For all data requests:

1. Requestor agrees to preserve the confidentiality of the Subject Data. Requestor agrees not to report or publish Subject Data in any manner that discloses individuals' identities in accordance with the Family Educational Rights and Privacy Act (FERPA), 34 CFR 99-31 (a) (6), and any applicable state laws, including, but not limited to, O.C.G.A. § 20-2-210, O.C.G.A. § 20-2-320, and 20-14-40. Requestor agrees not to publish any data or results derived from Subject Data for subgroups of students with an n-size less than 10. Requestor agrees not to make any effort to discover the identity of a subject.
2. Requestor shall not jeopardize the proprietary nature of the Subject Data by releasing, publishing, copyrighting, or otherwise publicly disseminating the Subject Data. However, Requestor may, subject to the terms of this Agreement, prepare reports or presentations using Subject Data.
3. Requestor agrees to use Subject Data only for the purpose identified by the Requestor in the application for data that was approved by the DMC, which is expressly incorporated by reference into this Agreement. Requestor agrees not to use Subject Data for any purpose other than what was identified by the Requestor in the application for data approved by the DMC. The Requestor's application is incorporated herein by reference. Any Caveats for Approval (if applicable) are also incorporated into this agreement.
    a. Any report or presentation that does not align with the original proposal is a material violation of the terms and conditions of this Agreement.
    b. Any report or presentation that does not align with the original proposal shall not be presented, published, or submitted for publication.
4. Requestor agrees not to use the data provided under the terms of this agreement for publication in either theses or dissertations.
5. Requestor agrees that any analysis containing data provided by the Georgia Independent College Association, hereinafter referred to as "GICA," will undergo a separate review and approval process by GICA personnel. GICA may prevent or revoke the use of their data at any time.

6. Requestor agrees to provide an electronic copy of each report or presentation, that Requestor produces using Subject Data, to GOSA at least 30 calendar days prior to presentation or submission for publication.
    a. Publications and reports of Subject Data and information related to it, including preliminary project descriptions and draft reports, shall involve only aggregate data and no personally identifiable information or other information that could lead to the identification of any individual.
    b. Requestor agrees to make changes required by GOSA that are necessary to prevent disclosure of personally identifiable information prior to presentation or submission for publication.
7. Requestor agrees to obtain written permission from GOSA in order to use the logo for GA•AWARDS.
8. Requestor agrees to include the following language in each report or presentation: "The contents of this report were developed using data provided by Georgia's Academic and Workforce Analysis and Research Data System (GA•AWARDS). However, those contents do not necessarily represent the policy of GA•AWARDS or any of its participating organizations, and you should not assume endorsement by GA•AWARDS or any of its participating organizations."
9. Requestor agrees not to merge or match the Subject Data with other data sources unless specified by the requestor and agreed to in writing by GOSA.
10. Requestor agrees that all Subject Data files, including derivative files and all data files resulting from merges or matches are subject to this Agreement. GOSA reserves the right to request all documents and files used to analyze the Subject Data.
11. Requestor agrees to complete a feedback survey and to provide additional feedback upon request.
12. GOSA may revoke this agreement at any time for cause or may cancel without cause on thirty (30) days written notice. Any violation of the terms and conditions of this Agreement may result in the immediate revocation of this Agreement by GOSA.
    a. GOSA may initiate revocation of this Agreement by written notice to Requestor indicating the factual basis and grounds of revocation.
    b. Upon receipt of the written notice of revocation, the Requestor shall immediately cease all research activity related to the Agreement until the issue is resolved. The Requestor will have three business days to submit a written response to GOSA indicating why this Agreement should not be revoked.
    c. GOSA shall decide whether to revoke the Agreement based on all available information. GOSA shall provide written notice of its decision to the Requestor within ten business days after receipt of the response. These timeframes may be adjusted for good cause.
13. Requestor understands that a violation of this Agreement will result in a material breach of contract and may subject the Requestor and his/her organization to prosecution under applicable laws. Requestor understands that a violation of this Agreement may affect the Requestor's ability to utilize private or protected data provided by GA•AWARDS in the future.
14. Requestor agrees to pay any and all fees as agreed upon.

15. Requestor agrees to limit and restrict access to those individuals listed on the application that have signed Confidentiality and Data Usage Agreements with GOSA.
    a. Requestor shall promptly notify GOSA in writing within one business day when an individual listed on the application has been terminated or access to individual-level data has been terminated and give the date thereof.
    b. Requestor agrees to notify GOSA immediately in writing within one business day upon receipt of any request or demand by others for disclosure of the Subject Data. Any such disclosure is prohibited unless specifically granted by GOSA in writing.
16. Requestor agrees to notify GOSA in writing immediately upon discovering any breach, or suspected breach, of security or any disclosure of Subject Data to an unauthorized party or agency.
17. Requestor agrees that the data provided under the terms of this agreement will remain within the United States and may only be accessed from within the United States.
18. Requestor agrees to retain the original version of the individual-level Subject Data on a secure server and shall not make a copy or extract of the Subject Data available to anyone except individuals specified in paragraph 15.
    a. Requestor agrees that all Subject Data when not on a Secure Server (14 b) must be encrypted in accordance with Federal Information Processing Standard 140-2 (FIPS 140-2) while in transit and at rest. GOSA will ensure the encryption of data in transit when it is retrieved from GOSA systems. The requestor is responsible for ensuring strong encryption in compliance with FIPS 140-2 during any other transmission of data, be it internal or external. Data at rest can be any data that are resident in a database or in a file that is stored on any media on any device. Files on mobile devices, including laptop computers, are considered data at rest and, due to the increased vulnerability to physical theft, must always be encrypted with strong encryption.
    b. Requestor agrees to secure Subject Data on a Secure Server. Secure Server may be construed to be any computer system where the practice of Security in Depth is applied. Security in Depth is defined as any redundant combination of access controls and deterrents that prevent unauthorized access to data, which include but are not limited to: robust user authentication, firewalls, intrusion detection, anti-virus and anti-malware, access logs and audits, and data loss prevention technologies. Security in Depth should be part of a comprehensive Information Security Management System (ISMS) in compliance with best practices described in ISO/IEC 27002. When it is deemed reasonable and appropriate to forgo a given control, the Requestor must provide written justification to GOSA that should include all the risk assessment factors considered when the decision was reached.
    c. Requestor certifies that the description of the ISMS provided in the application for data is true and accurate to the best of his/her knowledge and that he/she has achieved Security in Depth, as described above 14(b) as part of a ISO/IEC 27002 compliant best practices or that the requestor's environment is certified ISO 27001 compliant.

    Initial here: _____

d. GOSA recommends the use of an OpenPGP compatible cryptographic software to protect data both when in transit (over unsecured means) and at rest. GPG4Win is an OpenPGP and Microsoft Windows compatible implementation that has been vetted for this purpose. GPG4win is a no cost collection of cryptographic software that is available for use free of restrictions. GPG4Win relies on two main subcomponents. GnuPG is the main cryptographic library, which contains all of the functions to encrypt and sign files as necessary using FIPS 140-2 approved security functions RSA for encryption and SHA-1 for signing. Kleopatra is the key management software. It is Kleopatra with which the user will directly interface to manage (create, import, export) certificates. Please see http://www.gpg4win.org for details on usage and licensing.

19. Requestor agrees to destroy or return to GOSA individual-level Subject Data, and all media used to transfer it from GOSA to the Requestor, including all copies and derivative or merged files twelve months from the date this Agreement is signed by GOSA's Executive Director or forty-five (45) days after it is no longer needed to perform the study or research covered by this agreement, whichever occurs first. However, an extension may be granted by written agreement of the parties.
    a. GOSA and the Requestor shall work cooperatively to determine the proper medium and method for the transfer of confidential data between each other. The Requestor shall confirm the transfer of confidential data and notify GOSA as soon as practicable of any discrepancies between the actual data transferred and the data covered by this agreement. The same protocol shall apply to any transfer of confidential data from the Requestor to GOSA.
    b. Destruction of data should ensure that no portion of the subject data is recoverable or readable by any means readily available including for-hire data recovery and forensics services. If a data destruction service is used, a certificate of destruction from the service provider will be required as well.
    c. When data are stored on disposable media (e.g., CD, CDR, CDRW, DVD, DVD+/-R, DVDRW, Blu Ray, Blu Ray RW, floppy disk, etc.), the disposable media should be physically destroyed and the pieces disposed of by a secure trash collection facility.
    d. For data stored on magnetic media (e.g., traditional hard drive, tape, magneto optical, floppy disk, etc.) or USB thumb drives, the requestor must use a secure deletion software or file shredder set to a minimum of eight iterations or be physically destroyed as in 19(b). An example of software that performs this task is the ERASER software from http://eraser.heidi.ie/. Eraser is an advanced security tool for Windows that is free for use and licensed under the GPL http://www.fsf.org/licensing/licenses/gpl.html. The default operating settings are sufficient to comply with 19(c).
    e. For data stored on Solid State Drives (SSD), only SSD drives with TRIM support should be used, and the drive should be manually cleaned after the deletion of subject data. If this functionality is not available, the drive should be factory reset with the secure erase facility. Drives that do not support TRIM or secure erase should not be used for subject data or the drive should be physically destroyed as in 19(b).

20. Requestor agrees to sign the Certificate of Data Destruction and provide the signed Certificate to GOSA.
21. Requestor shall not assign or transfer the rights or obligations of this Agreement without the written consent of GOSA.
22. No modifications or alteration of this Agreement will be valid or effective unless each modification or alteration is made as an amendment to this Agreement and is signed by both parties.
23. If any provision of this Agreement is held to be invalid, illegal, or unenforceable for any reason, the validity, legality, and enforceability of the remaining provisions of this Agreement shall not be adversely affected.
24. This Agreement shall be deemed to have been executed in Fulton County, Georgia, and all questions of interpretation and construction shall be governed by the laws of the State of Georgia.
25. This Agreement may be executed in counterparts which, when taken together, will constitute one Agreement. Copies of this Agreement will be equally binding as originals and faxed or scanned and emailed counterpart signatures will be sufficient to evidence execution.

Jackie Lundberg Date	{Name} Date
Director of Data Systems and Operations, GOSA	Requestor