MEMORANDUM OF AGREEMENT
AMONG
NEW JERSEY DEPARTMENT OF EDUCATION,
NEW JERSEY DEPARTMENT OF LABOR AND WORKFORCE DEVELOPMENT,
OFFICE OF THE SECRETARY OF HIGHER EDUCATION
AND
RUTGERS, THE STATE UNIVERSITY OF NEW JERSEY, on behalf of the JOHN J. HELDRICH CENTER FOR WORKFORCE DEVELOPMENT

This Memorandum of Agreement (the "Agreement") is entered into by and between the New Jersey Department of Education ("NJDOE"), the New Jersey Department of Labor and Workforce Development ("NJDLWD"), the New Jersey Office of the Secretary of Higher Education ("OSHE") (collectively, "Data Owners") and Rutgers, the State University of New Jersey on behalf of the John J. Heldrich Center for Workforce Development ("Data Recipient"), in order to set forth the terms under which the Data Owners will share data with the Data Recipient to further the New Jersey Education to Earnings Data System (NJEEDS), in a manner consistent with applicable federal and State laws.

I. BACKGROUND

The NJDOE, NJDLWD and OSHE have entered into a Memorandum of Understanding, incorporated into this Agreement as Attachment A, to create NJEEDS, a statewide longitudinal data system to include Pre-school to grade 12 "P-12" education, higher education and labor/workforce data intended to enhance the ability of the State of New Jersey to efficiently and accurately manage, analyze, and use education, higher education and employment and workforce data, including individual records. NJEEDS is designed to help the State of New Jersey, districts, schools, participating postsecondary institutions, educators, workforce development professionals and other stakeholders make data-informed decisions to improve student learning and outcomes, as well as to facilitate research to increase student achievement and close achievement gaps. NJEEDS will be instrumental in defining and fulfilling the State's research agenda, which shall include but not be limited to, satisfying the State of New Jersey's respective commitments for the State Fiscal Stabilization Funds received through the American Recovery and Reinvestment Act (indicators (c)(11) and (c)(12), the America COMPETES Act, the Every Student Succeeds Act, the Annual Reports by Institutions of Higher Education (Institutional Profiles)(N.J.S.A.18A:3B-35), and the requirements of the Statewide Longitudinal Data System (SLDS) grant (U.S. Department of Education #R372A120025). It will also support the requirements

of two Workforce Data Quality Initiative grants awarded to NJLWD from the U.S. Department of Labor to develop a workforce longitudinal data system (WDQI MI-23214-12-60-A-34 and MI-25898-14-60-A-34).

II. DEFINITIONS

Unless otherwise specified in this Agreement, all capitalized terms used in this Agreement not otherwise defined shall have the meaning established by law as applicable to the relevant nature, source, and context of the data.

III. SCOPE AND PURPOSE

This Agreement sets forth the terms and conditions pursuant to which the Data Owners will transmit the data elements identified in Attachment B ("Data"), to the Data Recipient. Except as otherwise provided in another Data Use Agreement between Data Recipient and one or more of the Data Owners, Data Recipient may use the Data only for the purposes described in this Agreement.

It is the intention of the Parties that the Data transmitted by Data Owners be used by Data Recipient to i) establish, maintain and secure the NJEEDS, ii) perform data analytics for research projects that have first been approved by the Agencies under the procedures set forth in Attachment A to this Agreement, and iii) to manage the NJEEDS system as specified in Attachment A, including fulfilling Data Recipient's obligations to satisfy research projects approved by the Data Owners, as allowed by Section VI.4 of this Agreement.

IV. TERMS FOR SHARING OF DATA BY DATA OWNERS

1. In order to meet the needs of NJEEDS, the Data Owners agree to supply the Data Recipient with the Data on a regular basis, according to the data transfer schedules and methods developed by the Data Owners and Data Recipient, for the duration of this Agreement or until NJEEDS is terminated by the Agencies as defined in Attachment A. The Data Owners hereby represent and warrant that to the best of their knowledge, the Data is accurate and contains no known errors or misinformation.

2. The Data Owners and Data Recipient shall use the Data Transfer Requirements (as specified in Attachments A, B and C) to transfer the Data from each Data Owner to the Data Recipient. All Parties hereby acknowledge and confirm that the Data Transfer Requirements

meet or exceed the technical and privacy safeguards necessary for the Data.

3. The Data Owners agree that in order for the Data Recipient to establish and maintain NJEEDS, it will be necessary for Data Recipient to link the Data received from each Data Owner with data provided from other sources ("Other Data") in order to create a Linked Data Set.

V. SAFEGUARDING OF DATA BY DATA RECIPIENT

1. The Data Recipient shall store and maintain all Data obtained pursuant to this Agreement in a secure computer environment, including password protection and/or encryption of the data files, and shall comply with the specifications in the NJEEDS Data Safeguard document, attached and incorporated as Attachment C. Data Recipient shall store and process Data maintained in electronic format, such as magnetic tapes or discs, in such a way that unauthorized persons cannot obtain the information by any means. Data Recipient will not copy, reproduce or transmit data obtained pursuant to the Agreement except as allowed by this Agreement and its Attachments. All copies of data of any type, including any modifications or additions to data from any source that contains information regarding individuals, are subject to the provisions of the Agreement in the same manner as the original data.

2. All transmissions of the Data, whether between the Data Owners and the Data Recipient, or an approved third party, shall use encrypted and secure transmission methods in order to meet the technical and/or physical safeguards as may be required by law. The Parties hereby acknowledge and confirm that the data transfer requirements at Attachments A, B and C meet or exceed the technical and privacy safeguards necessary for the Data.

3. The Data Owners reserve the right to conduct inspections of the Data Recipient's facilities to verify that the specified controls are in place.

4. The Data Recipient agrees to not use or disclose the Data for any purpose other than in performance under this Agreement or as required by law.

5. The Data Recipient shall comply, in all respects, with the provisions of the Family Educational Rights and Privacy Act ("FERPA"). For purposes of this Agreement, FERPA includes all provisions of 20 U.S.C. §1232g, any amendments or other relevant

provisions of federal law, and all requirements of Chapter 99 of Title 34 of the Code of Federal Regulations. Nothing in this Agreement may be construed to allow any Party to maintain, use, disclose or share student information in a manner not allowed by federal law or regulation.

6. The Data Recipient shall comply, in all respects, with the requirements of 20 CFR Part 603 to prevent unauthorized use or disclosure of any personally identifiable information, unemployment insurance, wage and employer data. It shall maintain the confidentiality of such unemployment compensation data that reveals the name or any identifying particular about any individual or any past or present employer or employing unit, or which could foreseeably be combined with other publicly available information to reveal any such particulars and shall not disclose any such information except to authorized personnel for the express purposes as set forth in this Agreement.

7. All data exchange activity governed by this Agreement shall be conducted in accordance with the purpose of this Agreement and is to be bound by federal and state statutes, laws and regulations restricting the use and release of data or information conveyed pursuant to the purpose of this Agreement. The Data Recipient shall, in accordance with this Agreement, ensure that data is obtained through the appropriate administrative, technical, procedural, and physical safeguards and shall protect the confidentiality of such data and to prevent unauthorized access to it consistent with, at a minimum, the following federal and state statutes, laws, regulations and generally recognized industry standards:

a. 42 C.F.R. Part 2
b. Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, as implemented by 34 CFR Part 99.31(a)(3) and 99.35.
c. N.J.S.A. 44:10-47
d. Center for Internet Security—see http://www.cisecurity.org
e. National Institute for Standards and Technology—see http://csrc.nist.gov
f. Federal Information Security Management Act (FISMA)—see http://csrc.nist.gov
g. ISO/IEC 27000-series—see http://www.iso27001security.com/
h. Organization for the Advancement of Structured Information Standards (OASIS)—see http://www.oasis-open.org/
i. Open Public Records Act ("OPRA"), N.J.S.A. 47A:1A-1.1 et seq
j. 20 CFR Part 603
k. N.J.A.C. Title 12, Chapter 15, Subchapter 2 (Disclosure of Information)

8. The Data Recipient agrees to perform under this Agreement in such a manner that does not permit personal identification of individuals by anyone other than representatives of Data Recipient who need it to perform the official purposes recognized in this Agreement. All persons with access to personally identifiable information will be advised of the confidential nature of the information. Nothing in this Agreement authorizes sharing Data with any other person or entity for any purpose other than a person or entity specified within who is authorized to complete Data Recipient's work under the Agreement or is authorized under this Agreement.

9. The Data Recipient agrees not to disclose or publish any data obtained under this Agreement in a manner that could identify any particular individual. The Data Recipient also agrees not to use or attempt to use the Data in a manner to contact any particular individual. The Data Recipient will ensure that its agents and any subcontractors agree to abide by these provisions.

10. The Data Recipient will require and ensure that all of its employees, contractors and agents of any kind comply with all applicable provisions of FERPA, 20 CFR Part 603, and other federal and state laws with respect to the Data. All employees, contractors and agents of the Data Recipient with access to the Data shall be bound by the same restrictions and conditions that apply through this Agreement. The Data Recipient shall inform the respective Data Owner(s) of the sharing of that agency's Data with a subcontractor to further this Agreement thirty (30) days prior to doing so and will obtain the Data Owner's written consent in advance of allowing the agent or subcontractor access to the Data.

11. All Data no longer needed for purposes of this Agreement, and/or upon termination of this Agreement, shall be destroyed by Data Recipient using reasonable commercial methods. The Data Recipient agrees to require all employees, contractors or agents of any kind to comply with this provision. The Data Recipient shall provide each Data Owner with a certification attesting to the destruction of the Data.

12. With respect to education records from NJDOE and/or OSHE, the Data Recipient acknowledges that, pursuant to 20 U.S.C. §1232g(b)(4)(B), if it permits access to Data in violation of this Agreement or fails to destroy Data in violation of FERPA, it will be prohibited from accessing NJDOE/OSHE student records for a period of not less than five years.

13. The Data Recipient agrees to report, verbally and in writing, to the applicable Data Owner(s) within five (5) days of its discovery of any use or disclosure of the Data that is not provided for by this Agreement, including without limitation, any disclosure to an unauthorized subcontractor or third party.

The Data Recipient agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of personally identifiable information or other event requiring notification. In the event of a breach of any NJEEDS integrated data system data, security obligations, or other event requiring notification under applicable law, the Data Recipient shall:

a. Notify all Data Owners by telephone and e-mail of such an event within 24 hours of discovery;
b. Assume responsibility for informing all affected individuals in accordance with applicable laws; and
c. Hold harmless and defend Data Owners and their employees from and against any claims, damages or other harm related to such Notification Event. All costs associated with such Notification Event shall be the responsibility of the Data Recipient, including attorney fees and costs and court costs.

VI. ACTIVITIES AND OBLIGATIONS OF DATA RECIPIENT

1. The Data Owners hereby grant permission to the Data Recipient to use the Data to establish, maintain and secure the NJEEDS, in accordance with the terms of this Agreement and Attachments.

2. The Data Owners also hereby grant permission to the Data Recipient to use the Data to produce reports and/or analyses at the request of or on behalf of the State of New Jersey or Data Owners, under the procedures and terms set forth in this Agreement, its Attachments, and the NJEEDS Acceptable Use Guidelines, NJEEDS Data Access and Use Policy, and NJEEDS Data Access Request Process.

3. The Data Recipient will not share or in any way use data received by any Data Owner with any other entity unless the Data Recipient has first obtained the prior written approval of the Data Owner. It is understood by the Parties that the Data Owners shall not unreasonably withhold permission to share the Data with another entity if such request is permissible by law and is in furtherance of the mission of the NJEEDS. The Data Owners agree to review all Data requests submitted by the Data Recipient promptly and shall notify the Data Recipient within twenty (20) business days as to whether the request for access to the Data is

approved or denied. If the Data Owner does not respond to such Data request within thirty (30) business days of the submission of the request, the non-response shall be construed as a denial of the request.

4. The Data Owners and the Data Recipient shall establish a process through which authorized third parties, which may include Rutgers, The State University of New Jersey and may further include its John J. Heldrich Center for Workforce Development, may request access to the Data to facilitate or perform research. The Parties agree that in furtherance of the NJEEDS, the Data Recipient may share the Data with third party authorized users, as defined in the NJEEDS Acceptable Use Guidelines, and the NJEEDS Data Access and Use Policy, to further submitted research proposals, only with approval from the Data Owner(s) and using a Data Access Request Process to be established and agreed upon by the Data Owners and Data Recipient.

5. The Data Recipient will not share the Data with any other persons, entities, providers, or other sections or divisions of Rutgers, the State University of New Jersey, without the prior approval of the Data Owner(s). The Data Recipient will ensure that any approved third party user, including any additional Rutgers user, agrees to abide by the same restrictions and conditions as contained here and in the NJEEDS Acceptable Use Guidelines and NJEEDS Data Access and Use Policy before releasing the approved Data. The Data Recipient will not share the Data with any other persons, entities, providers or other sections or divisions of State Government, without the prior approval of the Data Owner(s).

6. The Data Recipient shall designate in writing a single authorized representative able to manage requests for Data under the Agreement. The authorized representative shall be responsible for maintaining a record of all Data requested and received pursuant to the Agreement, including confirmation of the completion of each research project and the return or destruction of Data as required by the Agreement. The Data Owners may upon request review the records required to be kept under this section.

VII. INDEMNIFICATION

The Data Recipient shall indemnify, defend, and hold harmless the Data Owners and all of the Data Owners' affiliates, and their respective trustees, officers, directors, employees, and agents from and against any potential or asserted claim, cause of action, liability, damage, cost, or expense (including without limitation,

the costs of investigation and settlement, and reasonable attorney's fees and court costs) arising out of or in connection with any unauthorized or prohibited use or disclosure of the Data by Data Recipient or its employees, contractors, and agents of any kind, or any other breach of this Agreement.

VIII. TERM AND TERMINATION

1. This Agreement will take effect upon signature by the authorized representative of each Party and will remain in effect for five (5) years from the date of execution and will automatically renew no more than three times for an additional one (1) year for each renewal.

2. Fully cognizant that the Data from each Data Owner is vital for the continued operation of NJEEDS, any Party may, nevertheless, terminate this Agreement for convenience with sixty (60) days written notice to the other Parties. Notwithstanding the above, the Data Owners reserve the right to terminate the Agreement should a Data Owner, in its sole discretion, determine that confidential information has been released in a manner inconsistent with the Agreement, or that the Data Recipient has not maintained Data in a secure manner consistent with the provisions of this Agreement.

3. Upon termination of the Agreement, the Parties shall exercise their best efforts to locate suitable storage and to transfer the Data maintained by the Data Recipient. The Data Owners and the Data Recipient shall work together to ensure that the Data is capable of being transferred in a secure and protected manner. All Data provided by the Data Recipient to an agent, including a subcontractor, shall be returned or destroyed upon termination of the Agreement.

4. Upon termination or expiration of this Agreement, the Data Recipient shall return or destroy the Data and ensure that all necessary protections are extended to any existing Data, to ensure that the Data is not disclosed to any entity. All Data provided by the Data Recipient to an agent, including a subcontractor, shall be returned or destroyed upon termination of the Agreement.

IX. MISCELLANEOUS

1. The Parties agree to take such action as is necessary to amend this Agreement, Attachments and/or the NJEEDS Acceptable Use Guidelines, NJEEDS Data Access and Use Policy, and the forthcoming NJEEDS Data Access Request Process from time to time as is

necessary for the Data Owners or the Data Recipient to comply with the law.

2. Any modifications to this Agreement, its attachments and the associated NJEEDS Guidelines, Policy and Process must be mutually agreed to by all Parties in writing. All Attachments to this Agreement are hereby referenced and incorporated into this Agreement.

3. Any Party may request changes or modifications to this Agreement. However, no such change or modification shall be effective unless incorporated in a written amendment executed by all Parties. The Parties acknowledge that the Attachments may be amended from time to time by the Parties through a separate agreement. Any amendment to an Attachment to this Agreement shall be incorporated into this Agreement and attached to it.

4. The Parties will follow the procedures set forth in the Attachments in good faith.

5. There are no intended third party beneficiaries to this Agreement. Without in any way limiting the foregoing, it is the Parties' specific intent that nothing contained in this Agreement gives rise to any right or cause of action, contractual or otherwise, in or on behalf of the individuals whose information is used or disclosed pursuant to this Agreement.

6. No provision of this Agreement may be waived except by an agreement in writing signed by the waiving Party. A waiver of any breach of non-compliance with any term or provision shall not be construed as a waiver of any other term or provision, or of any subsequent breach or non-compliance with the same term or provision. A waiver cannot be granted if it is determined that it violates the law.

7. The persons signing below represent and certify that each has the right and authority to execute this Agreement on behalf of their respective Party and no further approvals are necessary to create a binding agreement. All Parties hereby represent and warrant that they can fulfill the obligations of this Agreement and that nothing it contains violates any third party obligations any Party may have.

8. In the event of any conflict between the terms and conditions stated in this Agreement, including all Attachments incorporated into the Agreement, and those contained in any other agreement or understanding between the Parties, written, oral or implied, the

terms of this Agreement shall govern, unless otherwise stated by the other written agreement.

9. This Agreement shall be construed in accordance with and governed by the laws of the State of New Jersey.

10. The Data Recipient and Data Owners shall be excused from the performance period under this Agreement if a delay is caused by inclement weather, fire, flood, strike, or other labor dispute, acts of God, acts of governmental officials or agencies, or any other cause beyond the control of Date Recipient. The excusable delay is allowed for the period of time affected by the delay. If a delay occurs, the parties will revise the performance period or other provisions appropriate.

11. The Parties will attempt in good faith to resolve any disputes promptly by negotiations between representatives of the Parties who have authority to settle the dispute. The designated representatives of the Parties shall endeavor to meet at a mutually acceptable time and place within fifteen (15) days after the date a Party notifies another Party of a dispute and thereafter as often as they reasonably deem necessary to attempt to resolve the dispute. The designated representatives shall discuss the dispute and negotiate in good faith in an effort to resolve the dispute without the need for mediation or arbitration. During the course of such negotiations, the Parties shall endeavor to honor all reasonable requests made by one another for information and factual support for their respective positions so that each Party may be fully advised. The specified format for such discussions and information/documentation exchange shall be left to the discretion of the representatives. If the parties fail to resolve the dispute within six (6) months, the Parties shall then agree on the proper forum to bring any necessary action, including mediation and/or binding arbitration.

12. Data Recipient’s performance under this Agreement will be of the same standard utilized by other similarly situated public institutions of higher education.

13. The Parties shall maintain reasonable and adequate insurance coverage given their respective roles and obligations under this Agreement.

14. No Party shall use the name or trademarks of the other Parties, nor of any member of the other Party’s staff, in connection with any publicity without the prior written approval of the other Parties. This shall not include Data Recipient’s internal

documents, annual reports and databases which may be available to the public and which may identify the existence of is Agreement.

15. Data Recipient shall retain title to all equipment and supplies purchased, fabricated, and/or used by Data Recipient in furtherance of this Agreement.

16. If any provision of this Agreement is determined to be invalid or unenforceable, the parties will negotiate in good faith revisions to the provision that may be required in order to render it valid and enforceable. In the event the parties are unable to agree to new or modified terms, the remainder of this Agreement will not be affected thereby if capable of performance in the absence of the invalid or unenforceable provision(s).

17. Each Party intends that an electronic copy of its signature stored in a PDF software application format shall be regarded as an original signature and agrees that this Agreement can be executed in any number of counterparts, each of which shall be effective upon delivery and thereafter shall be deemed an original, and all of which shall be taken to be one and the same instrument, for the same effect if all Parties hereto had signed the same signature page.

[Signature Page to Follow]

IN WITNESS WHEREOF, the duly authorized representatives of the parties hereby execute this AGREEMENT as of the date first written above.

Rutgers, The State University of New Jersey

CM

Signature: [signature]
Name: Melissa L. Matsil, J.D.
Title: Director, Corporate Contracts
Date: June 30, 2017

New Jersey Department of Education

Signature: Kimberley Harrington
Name: Kimberley Harrington
Title: Acting Commissioner
Date: June 29, 2017

New Jersey Department of Labor and Workforce Development

Signature: [signature]
Name: Aaron R. Fichtner
Title: Commissioner
Date: June 29, 2017

New Jersey Office of the Secretary of Higher Education

Signature: [signature]
Name: Rochelle Hendricks
Title: Secretary of Higher Education
Date: June 29, 2017

Attachment A

MEMORANDUM OF UNDERSTANDING
AMONG
NEW JERSEY DEPARTMENT OF EDUCATION,
OFFICE OF THE SECRETARY OF HIGHER EDUCATION,
AND THE
NEW JERSEY DEPARTMENT OF LABOR AND WORKFORCE DEVELOPMENT

This Memorandum of Understanding (MOU) is entered into between the New Jersey Department of Education (NJDOE), the New Jersey Office of the Secretary of Higher Education (OSHE) and the New Jersey Department of Labor and Workforce Development (NJLWD).

Background

In partnering together, the NJDOE, OSHE and NJLWD each agree to expand the current NJDOE P-12 Statewide Longitudinal Data System (SLDS) to include higher education and labor/workforce data and create a secure, common data storage and reporting system. These systems are intended to enhance the ability of States to efficiently and accurately manage, analyze, and use education data, including individual student records. The SLDSs help states, districts, schools, educators, and other stakeholders to make data-informed decisions to improve student learning and outcomes; as well as to facilitate research to increase student achievement and close achievement gaps. The expanded SLDS will be instrumental in defining and fulfilling a research agenda that will help meet the State of New Jersey's respective commitments for the State Fiscal Stabilization Funds received through the American Recovery and Reinvestment Act (indicators (c)(11) and (c)(12)), the America COMPETES Act, the Annual Reports by Institutions of Higher Education (Institutional Profiles) (N.J.S.A. 18A:3B-35), and the requirements of the SLDS grant (U.S. Department of Education #R372A120025). Additionally, it will also support the requirements of two Workforce Data Quality Initiative (WDQI- MI-23214-12-60-A-34 MI-25898-14-60-A-34) grants awarded to NJLWD from the U.S. Department of Labor to develop a workforce longitudinal data system.

The expanded SLDS will facilitate data collection, storage and reporting from pre-kindergarten to high school, college, and through career. The extension of the existing SLDS platform, warehouse, and reporting structures will accommodate direct postsecondary institution uploads and the inclusion of workforce data via single source upload at select times throughout the year. The environments and databases housing data will, pursuant to this MOU, be separated appropriately and structured to ensure security and compliance with the Family Educational Rights and Privacy Act (FERPA); National Institutes of Standards and Technology (NIST) and related Federal Information Security Management Act (FISMA) security guidelines (where applicable); and state requirements related to the storage of sensitive education data elements and any data shared by NJLWD, including all Personally Identifiable Information (PII); relative to unemployment compensation data shared by NJLWD, each party to this MOU will ensure compliance with Section 303(a)(1) of the Social Security Act (SSA), Sections 303(a)(7), (c)(1), (d), (e), (h) and (i) of the SSA, Section 3304(a)(16) of the Federal Unemployment Tax Act (FUTA), and 20 CFR Part 603. Such partitioned sections of the SLDS guarantee that data are in

fact kept separate, empowering each Agency that provides data to maintain its individual agency governance and security protocols.

This memorandum uses as its foundation agreed-upon principles by which the partnering Agencies will conduct themselves for contributing and sharing data housed by the Agent. The specific roles, responsibilities, and procedures of the agencies for safeguarding and sharing data are detailed in this MOU.

Agreement

I. Purpose, Legal Authority and Definitions

A. Purpose

1. The purpose of this MOU is to establish agreement among NJDOE, OSHE and NJLWD to facilitate the exchange, transfer, or release of records as outlined in this MOU. This MOU will govern the terms under which the Agencies will provide Confidential Information to an Agent (to be designated by the Agencies), to match data on individuals across Agencies, and then de-identify the data to make it available for research purposes.

2. Confidential Information, including Personally Identifiable Information (PII), is required, and its use is addressed in this MOU to support fulfillment of the American Recovery and Reinvestment Act State Fiscal Stabilization Funds (indicators (c)(11) and (c)(12), the America COMPETES Act, Annual Reports by Institutions of Higher Education (Institutional Profiles) (N.J.S.A. 18A:3B-35), and the requirements of the Statewide Longitudinal Data Systems (SLDS) grant from the U.S. Department of Education requiring the NJDOE and OSHE, respectively, to accomplish the linking and analysis of information across state agencies to better inform educational policy alignment and satisfy public reporting requirements.

3. Attached to this MOU as Exhibit A is the MOU signed by the agencies on February 4, 2015, hereafter referred to as the "Governance MOU," the stated purpose of which is to establish a working relationship among NJDOE, OSHE and NJLWD in order to establish the P-20W data governance program to oversee the development and use of the P-20W-SLDS.

4. This agreement shall, among other things, establish the operating conditions and procedures that will govern actions of the agencies, the P-20W Warehouse Agent and other Agents holding Unemployment Insurance Wage data and workforce development case management data and establish certain conditions and procedures, consistent with 20 CFR Part 603, that are intended to protect the confidentiality of information disclosed by NJLWD to the Agencies, the P-20W Warehouse Agent and other Agents.
5. Participating Agencies shall provide data necessary for conducting a match among data sets to evaluate both P-12 and postsecondary education programs and assess the degree to which education programs are preparing students for postsecondary education and the workforce and for other audit and evaluation activities as defined under FERPA.

B. Legal Authority

1. The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) protects the privacy of student education records maintained by or for educational agencies or institutions that receive funds from the U.S. Department of Education.

    a. FERPA generally bars disclosure of education records without written parent or eligible student consent unless the disclosure comes within a list of authorized disclosures in the law.

    b. The regulations are designed to foster more comprehensive use of individual data for educational research, evaluation, accountability, and improvement purposes, while enhancing privacy protections and enforcement.

    c. This MOU will ensure consistency with federal and state laws as they relate to the management and handling of data, including confidential and Personally Identifiable Information as it is defined in FERPA.

2. The regulations issued pursuant Section 303(a)(1) of the Social Security Act (SSA), Sections 303(a)(7), (c)(1), (d), (e), (h) and (i) of the SSA, Section 3304(a)(16) of the Federal Unemployment Tax Act (FUTA)and codified at 20 CFR Part 603 govern the Confidentiality and Disclosure of State Unemployment Compensation Information. Each Agency and their Agent is responsible for complying with the provisions of 20 CFR Part 603 and with the related provisions of this MOU relative to its access to and use of State Unemployment Compensation Information.

3. This MOU works within the Governance structure defined in the Memorandum of Understanding signed by the NJ DOE, the NJ OSHE, and the NJLWD departments for the State Longitudinal Data System. See Exhibit A.

C. Definitions

1. "Personally Identifiable Information" or "PII" includes, but is not limited to, a person's name; parent or family member name; address; personal identifiers, such as social security numbers or student numbers; other indirect identifiers, such as date of birth, place of birth and; any other information that, alone or in combination, is linked or linkable to a specific person that would allow a reasonable person in the community, who does not have personal knowledge of the relevant circumstances, to identify the person with reasonable certainty; information requested by a person who the Agency reasonably believes knows the identity of the person to whom the record relates, as defined in 34 C.F.R. § 99.3; or any other information deemed personally identifiable by any applicable State or federal law or regulation as specified above .

2. "Confidential Information" means any and all information obtained from NJDOE, OSHE and/or NJLWD pursuant to this MOU or previous agreements and includes, but is not limited to, Personally Identifiable Information as explained above, Workforce, K-12 and Higher Education records, information about employees, benefit amounts and history, unemployment insurance payments, unemployment claims, employer history, salaries, wage histories, addresses, telephone numbers, bank account information, federal employer identification numbers, NAICS and industry codes, work histories, and social security numbers, including Unemployment Insurance Wage data and workforce development case management data. "Confidential information" does not include information that is aggregated so that the identity of a single person cannot be discerned and from which no Personally Identifiable Information ("PII") about any individual or any employing unit can be ascertained, either in isolation or when considered with other aggregated data to identify an individual.

3. "Agency" means NJDOE, OSHE or NJLWD. "Agencies" means NJDOE, OSHE and NJLWD.

4. "Agent" means the contracted vendor(s) of any of the participating Agencies that is involved in the collection or handling of data related to this MOU.

5. "Records" means recorded individual-level information derived in whole or in part from the information received from NJDOE, OSHE or NJLWD pursuant to this MOU, regardless of the format of the information and regardless of whether the information is an original or a copy. Records may include confidential information. A single record at an individual level is also known as a "unit record." Information which is aggregated above the individual level and excluded from the definition of "Confidential Information" is not included in this definition of "records".

6. "Re-disclosure" means transfer or disclosure of Confidential Information to any other person or entity whose access to Confidential Information is not specifically authorized, even if that person or entity has a contractual relationship with the Agencies.

7. "Cross-agency" indicates that information from more than one Agency is included as applicable to data, records, reporting, and research.

8. "P-20W Data" includes data from pre-kindergarten (early childhood education), K-12, postsecondary through post-graduate education, along with workforce data.

9. "P-20W Warehouse" is the common data repository where records obtained from NJDOE, OSHE and NJLWD and forming the SLDS is stored and used for cross-agency reporting.

10. "P-20W Warehouse Agent" is the agent or entity that will house the P-20W Warehouse data repository. The Warehouse agent may be an agency, another State or federal Government entity, or may be determined via the State's procurement and contracting process. The state may also opt, at its discretion to own the data warehouse. Presently the P-20W Agent, pursuant to New Jersey State Contract T-2302, is Public Consulting Group.

11. "De-identified data" refers to the process of removing or obscuring any personally identifiable information from records in a way that minimizes the risk of unintended disclosure of identity of individuals and information about them, and shall meet the requirements of any applicable law, including FERPA.

12. "Recipients" are any persons or entities requesting or receiving cross-agency records governed by this this MOU and in compliance with Federal and state laws and the policies for data sharing to be established by the Data Advisory Council.

13. "P-20W Data Advisory Council" is the governing group, established by the February 4, 2015 MOU between the Parties, and charged with developing and carrying out the research agenda and other activities under the SLDS and USDOL Workforce Data Quality Initiative grants.

14. "P-20W Data Steward Workgroup" is the workgroup established between the Parties responsible for ensuring the availability of the data required to carry out the research agenda approved by the Data Advisory Council, established by the MOU found in Exhibit A as well as other deliverables required for the SLDS and USDOL Workforce Data Quality Initiative grants.

15. The "NJDOE P-12 Statewide Longitudinal Data System" or ""SLDS" is a system intended to enhance the ability of states to efficiently and accurately manage, analyze, and use education data, including individual student records. It allows states, districts, schools, educators, and other stakeholders to make data-informed decisions to improve student learning and outcomes; as well as to facilitate research to increase student achievement and close achievement gaps.

II. Systems Operations/Data Processing Responsibility

1. Each Agency and/or its Agent(s) will provide read only access to data housed within the SDLS and transferred from the following systems: The Student Unit Record (SURE) system designed to strengthen the capacity of New Jersey Higher Education to discharge its research, planning, and coordinating responsibilities, and to assist institutions in a variety of ways, NJSMART, a system designed to provide data quality and capacity needed to build systemic and sustained data use at the state, district, school, and classroom levels. Workforce Development case management data and Unemployment Insurance (UI) Wage Records to the P-20W Warehouse Agent as well as any data from other systems that be identified as necessary in the future by the Data Advisory Group. The data shared will include Confidential Information, with the exception of data elements that an Agency determines to be irrelevant for accomplishing research objectives, or that the sharing thereof is a violation of a any applicable State or Federal law.

2. Electronic transfer of data will be provided through a secure data transfer method. The State of New Jersey has contracted for Data Motion to provide secure data transfer services for all state agencies. Data transferred pursuant to this agreement will take place through Data Motion's secure data transfer portal in accordance with the protocols established by the New Jersey Office of Information Technology.

3. The Agencies agree that direct access to NJDLWD, NJDOE, and OSHE data stored in the P-20W Warehouse shall be restricted to Agency staff and Agents authorized by these agencies in writing and approved by the Data Advisory Council.

4. The Agencies will ensure that
    a. the P-20W Warehouse Agent will store the de-identified data from the Agencies using the high level of encryption methodology; and

    b. access to data is password protected, at a minimum, in accordance with protocols established by the Office of Information Technology.

5. The Agencies agree that, if this MOU is terminated or suspended for any reason, the Agencies will immediately direct their Agents to cease all disclosures to the P-20W Warehouse Agent pursuant to this MOU, until such time as the MOU is reinstated or a new MOU is put into place.

6. The parties each acknowledge that each Agency retains ownership of the data that it contributes to the P-20W Warehouse whether through its authorized staff or an Agent(s).

7. Pursuant to 20 CFR 603.8, under no circumstances shall funds granted to NJLWD by the federal government for administration of the Unemployment Compensation program be spent to pay any of the costs associated with this MOU, including any costs associated with the disclosure of Unemployment Compensation information.

8. Agencies understand and agree that no PII shall under any circumstances be shared with or re-disclosed to any individual who is not a party to this MOU or to any entity which is not a party to this MOU. The Agencies further understand and agree that as a precondition to the sharing or re-disclosing of Confidential Information with/to an individual who is not a party to this MOU or to any entity which is not a party to this MOU, there must first be in place a data sharing agreement between and amongst the Agency whose Confidential Information is being shared or re-disclosed, and the recipient of the Confidential Information.

III. Duration, Modification and Termination of MOU

A. Duration

1. This MOU will be effective upon signature by an authorized representative of each Agency.

a. This MOU will expire on June 30, 2017, but may be extended for up to 5 additional 2 year terms upon the written agreement of all parties

b. The renewal of this MOU is contingent on each Agency participating in the renewed data sharing arrangement.

B. Modification

If the participating Agencies jointly determine that a modification of this MOU is necessary to comply with any new or amended state or federal requirements, then:

1. The Agencies may modify this MOU in writing at any time.

2. Modifications to the MOU shall be approved and signed by the Agency heads or their designated representatives.

IV. Termination

This MOU shall remain in force and effect until June 30, 2017, unless it is terminated by any of the following provisions:

1. If this MOU is found by a court or tribunal of competent jurisdiction to be in conflict with any United States or New Jersey statute or with any rule, regulation, guideline or directive of the U.S. Departments of Education or Labor, or regulation of the State of New Jersey, it shall be null and void to the extent of the conflict.

2. Any Agency may unilaterally terminate this MOU upon written notice to the other Agencies, in which case the MOU will terminate either 30 days after notice is sent, or at a date specified in the notice, whichever is later. This MOU may be terminated at any time by the mutual written consent of all Agencies.

3. In the event of termination, all records containing confidential information in the P-20 Warehouse shall immediately cease to be used and shall be returned to the contributing Agency in accordance with the terms of the Agent's contract. In the alternative, the records containing Confidential information in the P-20 Warehouse may be destroyed and the entity responsible for the destruction shall certify to the destruction. The Agencies responsible for the contract with the Agent for the P-20 Data Warehouse

shall ensure that Agents comply with cessation directions, return or destruction of records, and any certifications.

4. This MOU may be terminated in in the event that funds necessary for its execution are either not appropriated by the Legislature or are not available.

5. Nothing in these provisions shall prevent an Agency from terminating this MOU on less than 30 days' notice if the Agency determines the safeguards outlined herein are not adhered to and there is imminent risk that records containing Confidential Information have been or are endanger of used or disclosure.

V. Procedures for Security

The parties agree to safeguard all Confidential Information as follows:

1. Confidential Information will be used only as authorized by this MOU.

2. Access to Confidential Information will be restricted to only those Agency employees and Agents who need access to perform the duties and obligations recognized in this MOU.

3. Confidential Information will at all times be stored in a manner that is physically safe from access by unauthorized persons. Confidential Information that is maintained in electronic format will be stored in such a way that unauthorized persons cannot obtain the information by any means.

4. All persons with access to Confidential Information will be advised of the confidential nature of the information, the safeguards required to protect the Confidential Information, and the civil and criminal sanctions for noncompliance contained in applicable New Jersey and federal laws. Prior to disclosure, an authorized representative of each Agency shall sign an acknowledgment stating that all applicable persons have been instructed in accordance with this subsection. Additionally, each Agency will require all persons with access to Confidential Information to sign a written acknowledgement stating that he/she has been instructed in accordance with this subsection and maintain them on file for audit by any of the other agencies.

5. Any unauthorized disclosure or re-disclosure of Confidential Information learned of by any Agency must be reported to the providing agency on the same business day or if not possible, on the next business day be reported to

the Agency that provided the data and promptly reported in writing to the Data Advisory Council.

6. In the event that any equipment or records containing Confidential Information are transported from one location to another in furtherance of the purpose of this MOU, the transporting Agency or its agent will take all necessary steps to ensure that the information is transferred in a way that maintains the confidentiality safeguards of this MOU and in accordance with protocols established by the Office of Information Technology.

7. All computers and other electronic devices and media containing Confidential Information will be encrypted and/or password protected in accordance with protocols established by the Office of Information Technology.

8. Every person accessing Confidential Information must ensure compliance with this MOU, with all modifications or amendments to this MOU, and with all applicable state and federal statutes and regulations, including applicable amendments.

9. Each Agency will notify the Data Steward Workgroup of any major change in system platform (hardware and/or software) procedure and/or policy affecting transmission and/or distribution of information occurring any time after this MOU is signed.

VI. Audits

Agencies agree to the following:

1. To allow audits to be conducted by one of the Agencies, or by any State or federal agency with oversight over one or all of the Agencies, any federal agencies with oversight of the Agencies, or any other entity required or permitted to audit the Agencies or the P-20W Warehouse, to ensure that the confidentiality requirements of this MOU and all applicable laws and regulations, including applicable amendments, are being satisfied. In the event an Agency requests the audit, the audit(s) will be conducted by an appropriate entity designated by the Agency requesting the audit.

2. To implement, within a reasonable time, recommendations pursuant to the audit authorized by this section. This section does not prohibit an Agency from suspending or terminating this MOU if a breach is discovered or suspected. The Agencies agree to determine whether the MOU should be suspended or terminated, or whether audit recommendations should be imposed.

3. If, as a result of the audit conducted pursuant to this section, an Agent is required to spend additional time addressing compliance with this MOU and according to contract terms, the Agency responsible to oversee Agent's performance will be responsible for the costs associated with these changes, with the exception that, pursuant to 20 CFR 603.8, under no circumstances shall funds granted to NJLWD by the federal government for administration of the Unemployment Compensation program be spent to pay any of the costs of making any disclosure of UC information, including costs associated with making changes to the system contemplated by this MOU in order to ensure compliance with State or federal confidentiality requirements or in order to ensure compliance with any audit findings.

4. To regularly monitor those persons with access to Confidential Information to determine whether the job responsibilities of those persons continue to require access, to immediately remove access for any person who is determined to no longer need it, and to take all necessary steps to ensure that any records which are in the possession or control of such persons are timely destroyed as provided in this MOU.

VII. Records Usage, Duplication, and Re-disclosure Restrictions

Agencies agree:

A. The Agencies agree to the following limitations on the use, duplication, and re-disclosure of Confidential Information:

1. That they will not re-disclose any Confidential Information to any other agency, entity, contractor, or person without explicit written authorization from the Agency providing the data and approval from the Data Advisory Council.

2. That they will not allow the duplication or dissemination of Confidential Information within their own organizations, except as necessary to fulfill the stated purpose of this MOU.

B. To adopt policies and procedures to ensure that all Confidential Information is used solely as authorized by this MOU and to ensure that the confidentiality of such information is safeguarded as required by federal and state law and regulations. These policies and procedures shall be available for review at any time requested.

C. That, if any violations or suspected violations of this MOU pertaining to the use, duplication, or re-disclosure of Confidential Information are discovered by any

Agency, that Agency will report such violations to the Agency providing the data immediately, where possible, and in all cases within two working days of the discovery of the violation.

VIII. Choice of Law

Any disputes arising under this MOU shall be governed by the laws of the State of New Jersey.

IX. Criminal penalties

The Agencies acknowledge that they, and their employees, are subject to criminal penalties for failure to comply with federal and state laws requiring that information be kept confidential and prohibiting the unauthorized re-disclosure of Confidential Information.

X. Civil Penalties

The Agencies acknowledge that they, and their employees, are potentially subject to civil penalties for failure to comply with federal and state laws requiring that information be kept confidential and prohibiting the unauthorized re-disclosure of Confidential Information. These penalties may include the withholding and loss of eligibility for applicable program funding.

XI. Severability of Provisions

In the event that any provision of this MOU is found to be inoperative, unenforceable, void, or invalid by any court or tribunal of competent jurisdiction, such provision is considered severable, and such finding shall not affect the validity, enforceability, or operation of any other provisions of this MOU.

XII. Persons to Receive Notices

The Agencies agree to provide all formal and informal notices under this MOU to the persons listed below and to notify the other Agencies of any changes to the below.

A. New Jersey Department of Education contact is:

Bari Anhalt Erlichson
Assistant Commissioner

(609) 341-3142
bari.erlichson@doe.state.nj.us

B. Office of the Secretary of Higher Education contact is:

Elizabeth (Betsy) Garlatti
Chief of Staff
(609)-292-3235
Elizabeth.Garlatti@oshe.nj.gov

C. New Jersey Labor and Workforce Development contact is:

Tiffany Smith
Principal Managing Analyst
(609)-292-0021
Tiffany.Smith@dol.state.nj.us

XIV. Signatures

This MOU is effective upon the signature of all of the authorized representatives listed below.

New Jersey Department of Education

David Hespe
Commissioner of Education

June 26, 2015
Date

Bari Anhalt Erlichson
NJDOE SLDS Representative

June 26, 2015
Date

Office of the Secretary of Higher Education

Rochelle Hendricks

Rochelle Hendricks
Secretary of Higher Education

June 26, 2015
Date

Elizabeth S. Garlatti

Elizabeth S. Garlatti
OSHE SLDS Representative

June 26, 2015
Date

New Jersey Department of Labor and Workforce Development

Harold Wirths
Commissioner

June 26, 2015
Date

Tiffany Smith
NJLWD SLDS Representative

6/26/15
Date

Exhibit A

MEMORANDUM OF UNDERSTANDING
AMONG
NEW JERSEY DEPARTMENT OF EDUCATION,
OFFICE OF THE SECRETARY OF HIGHER EDUCATION,
AND THE
NEW JERSEY DEPARTMENT OF LABOR AND WORKFORCE DEVELOPMENT

This Memorandum of Understanding (MOU) is entered into between the New Jersey Department of Education (NJDOE), the New Jersey Office of the Secretary of Higher Education (OSHE) and the New Jersey Department of Labor and Workforce Development (NJLWD).

Background

In partnering together, the NJDOE, OSHE and NJLWD each agree to establish a P-20W data governance program in order to facilitate the expansion of the current NJDOE P-12 Statewide Longitudinal Data System (SLDS) into a P-20W SLDS that will include higher education and labor/workforce data, and create a secure, common data storage and reporting system.

The role of the P-20W data governance program will be to cultivate and establish a shared research agenda by identifying and defining 'data use deliverables' that would benefit both the state and stakeholders. The specific roles, responsibilities, and procedures of the agencies for establishing the P-20W data governance structure are detailed in this MOU. Pursuant to the framework established in this MOU, additional MOUs for this initiative will be executed, as needed, in order to implement data sharing and to govern the sharing of specific data files or data elements among the partner agencies. That is, no data or records obtained from NJDOE, OSHE or NJLWD, will either be shared amongst the agencies or their agents or stored in a warehouse, without execution of a subsequent agreement(s), separate and apart from this MOU, which agreement(s) would be signed by each of the agency heads.

Agreement

I. Purpose and Definitions

A. Purpose

The purpose of this MOU is to establish a working relationship among NJDOE, OSHE and NJLWD in order to establish the P-20W data governance program to oversee the development and use of the P-20W SLDS. Determinations made pursuant to this MOU by the Data Advisory Council or the Data Steward Workgroup shall not be binding on the Agencies; such determinations will be solely of an advisory nature and the adoption of any determination made pursuant to this MOU by an Agency shall be effectuated pursuant to that Agency's respective governance structure.

B. Definitions

1. "Agency" means either NJDOE, OSHE or NJLWD. "Agencies" means NJDOE, OSHE and NJLWD.

2. "P-20W" means data from prekindergarten (early childhood), K12, and postsecondary through post-graduate education, along with workforce and other outcomes data (e.g., public assistance and corrections data).

3. "Recording secretary" means the SLDS Project Director or the SLDS Project Director's designee.

4. "Warehouse" means the common data repository where records obtained from NJDOE, OSHE and NJLWD are stored and used for cross-sector reporting.

II. The P-20W data governance program

The P-20W data governance program collectively refers to the bodies with responsibility for advising the Agencies on the establishment and enforcement of policies involving data stored in the Warehouse. The P-20W data governance program shall be organized as a two-tiered structure consisting of a Data Advisory Council and a Data Steward Workgroup.

A. Agencies agree as to the Data Advisory Council (the Council):

1. The Council's mission will be to provide guidance and strategic direction for the P-20W data governance program. The Council will be responsible for making recommendations for the establishment of policies involving data stored in the Warehouse. These policies may include but are not limited to: the establishment of the data request process; data sharing protocol; supervision of data management for the P-20W SLDS, and determining which data elements will be both included in and provided from the Warehouse. Furthermore, the Council will establish a shared research agenda by identifying and defining data use deliverables to be completed by the Agencies.

2. The Council will be co-chaired by the NJDOE, OSHE, NJLWD Agency heads or representatives appointed by the respective Agency heads. NJDOE will serve as the secretary to the Council for administrative and convening purposes.

3. The Council will be comprised of four (4) representative stakeholders for each agency. The Agency Co-Chairs will represent their Agencies and each Co-Chair will designate three (3) representatives to the Council from key stakeholder groups. The representatives designated from stakeholder groups may include persons from school districts, higher education institutions, providers of workforce development programs, in addition to members of the community, researchers, and policy makers. There will be a total of twelve (12) members on the Council.

4. The Agency Co-Chairs will be the sole voting members on the Council. Decisions by the Agency Co-Chairs must be unanimous in order to be adopted by the Council. All decisions will be in compliance with federal and state regulations.

5. The Council will meet no less than four (4) times per year. All members of the Council will attend the meetings in person. At the first meeting held by the Council a meeting schedule for the next twelve (12) months will be adopted by the Agency Co-Chairs. The Council may also convene special meetings upon a unanimous decision to convene such a meeting. The recording secretary will record the minutes of each meeting and will provide the meeting minutes to the Agency Co-Chairs for approval within ten (10) days of the meeting. Upon receipt of the meeting minutes, the Agency Co-Chairs will have a 20-day period in which to either approve or reject the meeting minutes in writing to the recording secretary:

   (a) If no action is taken by an Agency Co-Chair within the 20-day period then the meeting minutes will be deemed approved by that Agency Co- Chair;

   (b) If an Agency Co-Chair rejects the meeting minutes then the basis for the rejection must be provided in writing to the other Agency Co-Chairs and the recording secretary, and the Agency Co-Chairs will attempt within 30 days of the notification of the rejection to address the basis for the rejection and to reach a unanimous decision on the contents of the meeting minutes. If a unanimous decision has not been reached by the date of the next scheduled Council meeting, then the matter of the approval of the meeting minutes will be scheduled by the recording secretary as the first agenda item for the next scheduled Council meeting.

   (c) Once the meeting minutes have been approved by the Agency Co- Chairs, the recording secretary will provide all members of the Council with a copy of the approved meeting minutes within three (3) working days.

6. At the first meeting held by the Council, the Council will consider whether to appoint a committee to draft by-laws for the Council and the Data Steward Workgroup. Any committee so appointed shall contain an equal number of representatives from each Agency.

B. Agencies agree as to the Data Steward Workgroup (the Workgroup):

1. The mission of the Workgroup will be to ensure the availability of data in the Warehouse needed to complete the research agenda and data use deliverables that will be determined by the Council.

2. The Workgroup will include four (4) representatives for each Agency. The members of the Workgroup will be selected by each Agency's Data Advisory Council Co-Chair. The members of the Workgroup must either be Agents or employees of the respective Agencies or submitters of data to the respective Agencies. There will be a total of twelve (12) Workgroup members. NJDOE will serve as the secretary to the Workgroup for administrative and convening purposes.

3. Workgroup members must have a thorough understanding of: (1) the policies and programs represented by the data in their Agency or organization; (2) the data collected by their Agency or organization, including definitions; and (3) the confidentiality requirements of federal and state law applicable to the data provided by their Agency.

4. The purposes of the Workgroup will be, under the general supervision of the Council: (1) to provide the most appropriate data from their Agency sources that support the accurate and effective implementation of the Warehouse; (2) to provide expertise in the content, context and availability of their agency/organization's data; and (3) to provide guidance to the Council on the structure of the Warehouse.

5. Members of the Workgroup will be expected to: (1) notify the Workgroup about issues that need to be addressed and help to propose resolutions for those issues; (2) provide data analysis in furtherance of Warehouse development and improvement; (3) communicate data quality issues identified by the Workgroup to their respective Agency; (4) communicate to the Workgroup any Agency data system changes and their potential impact on the Warehouse; (5) communicate to their respective Agency any Warehouse changes and their potential impact upon the Agency system; (6) attend Workgroup sessions in person or send a designated representative.

6. General direction and guidance for the Workgroup will be provided by the Council. For issues presented pursuant to paragraph five (5) of this section, the Workgroup will attempt to come to a decision as to an appropriate resolution. If a unanimous decision cannot be made, the meeting minutes will reflect all suggested resolutions and the issue will be escalated to the Council to be addressed at the next Council

meeting unless, at the request of the Workgroup, the Council elects to consider the issue in an expedited manner.

7. The Workgroup will meet no less than six (6) times per year. At the first meeting held by the Workgroup a meeting schedule for the next twelve (12) months will be determined and included in the meeting minutes. The Workgroup may also convene special meetings upon a unanimous decision to convene such a meeting. The recording secretary will record the minutes of each meeting and will provide the meeting minutes to the Workgroup members for approval within 10 (ten) days of the meeting. Upon receipt of the meeting minutes, the Workgroup Members will have a 10 (ten) day period in which to either approve or reject the meeting minutes in writing to the recording secretary:

   (a) If no action is taken by a Workgroup member within the ten (10) day period then the meeting minutes will be deemed approved by that Workgroup member;

   (b) If the meeting minutes are not unanimously approved by the Workgroup members, then the matter of the approval of the meeting minutes will either be scheduled as the first agenda item for the next scheduled Workgroup meeting or the Workgroup can, by majority decision, convene a special meeting to address the approval of the meeting minutes.

   (c) Once the meeting minutes are approved, the recording secretary will provide all members of both the Workgroup and the Council with a copy of the approved minutes within three (3) working days.

   (d) Upon the receipt of the meeting minutes by the Agency Co-Chairs of the Council, the Agency Co-Chairs will review all unanimous decisions made by the Workgroup pursuant to paragraph six (6) of this section. An Agency Co-Chair will notify the Secretary within 30 days of receipt if the Agency Co-Chair rejects any unanimous decision made by the Workgroup and will provide the basis for the rejection in writing to the recording secretary. The recording secretary will include the rejected matter for discussion and reconsideration as an agenda item for the next scheduled Workgroup meeting.

III. Duration, Modification and Termination of MOU

A. Duration

This MOU will be effective upon signature by an authorized representative of each Agency.

1. This MOU will expire on June 30, 2016.

2. The renewal of this MOU is contingent on each Agency participating in the P-20W data governance program.

B. Modification

If the participating Agencies jointly determine that a modification of this MOU is necessary, then:

1. The Agencies may modify this MOU in writing at any time, and such modifications will immediately be incorporated into this MOU.

2. Modifications to the MOU shall be approved and signed by the Agency heads or their designated representatives. Modifications to the MOU shall become effective upon signing by all respective Agency representatives or as otherwise stated in the modification.

C. Termination

This MOU shall remain in force and effect until June 30, 2016, unless it is terminated by any of the following provisions:

1. If this MOU is found by a court or tribunal of competent jurisdiction to be in conflict with any United States or New Jersey statute or with any rule, regulation, guideline or directive of the U.S. Departments of Education or Labor, or regulation of the State of New Jersey, it shall be null and void to the extent of the conflict.

2. Any Agency may unilaterally terminate this MOU upon written notice to the other Agencies, in which case the MOU will terminate either 30 days after notice is sent, or at a date specified in the notice, whichever is later. This MOU may be terminated at any time by the mutual written consent of all Agencies.

IV. Compliance with Applicable Law

The Agencies acknowledge that they, and their employees will comply with all applicable federal and state laws, including but not limited to the Family Educational Rights and Privacy Act (FERPA); the National Institutes of Standards and Technology (NIST) and related Federal Information Security Management Act (FISMA) security guidelines (where applicable); and state requirements related to the storage of sensitive education data elements and any data shared by NJLWD. Any agreements for the sharing of data, to the extent that it/they would involve the sharing or storage of Unemployment Compensation (UC) information, as that term is defined at 20 CFR 603.2(j), would contain each of the elements of an agreement for the sharing of confidential UC information required under 20 CFR 603.10.

V. Choice of Law

Any disputes arising under this MOU shall be governed by the laws of the State of New Jersey.

VI. Criminal penalties

The Agencies acknowledge that they, and their employees, are subject to criminal penalties for failure to comply with federal and state laws requiring that information be kept confidential and prohibiting the unauthorized re-disclosure of Confidential Information.

VII. Civil Penalties

The Agencies acknowledge that they, and their employees, are potentially subject to civil penalties for failure to comply with federal and state laws requiring that information be kept confidential and prohibiting the unauthorized re-disclosure of Confidential Information. These penalties may include the withholding and loss of eligibility for applicable program funding.

VIII. Severability of Provisions

In the event that any provision of this MOU is found to be inoperative, unenforceable, void, or invalid by any court or tribunal of competent jurisdiction, such provision is considered severable, and such finding shall not affect the validity, enforceability, or operation of any other provisions of this MOU.

IX. Persons to Contact

A. New Jersey Department of Education contact is:

Michael A. Keith, Jr.
P-20W SLDS Data and Policy Analyst
(609) 292-4336
Michael.Keith@doe.state.nj.us

B. Office of the Secretary of Higher Education contact is:

Elizabeth (Betsy) Garlatti
Chief of Staff
(609) 292-3235
Elizabeth.Garlatti@oshe.nj.gov

C. New Jersey Labor and Workforce Development contact is:

Tiffany Smith
Principal Managing Analyst
(609) 292-0021
Tiffany.Smith@dol.state.nj.us

X. Signatures

This MOU is effective upon the signature of all of the authorized representatives listed below.

New Jersey Department of Education

David Hespe
Commissioner of Education

1-29-15
Date

Bari Anhalt Erlichson
NJDOE SLDS Representative

1-22-15
Date

Office of the Secretary of Higher Education

Rochelle Hendricks
Secretary of Higher Education

1-30-15
Date

Elizabeth S. Garlatti
OSHE SLDS Representative

1-30-15
Date

New Jersey Department of Labor and Workforce Development

Harold Wirths
Commissioner

2/4/15
Date

Tiffany Smith
NJLWD SLDS Representative

1-30-15
Date

ATTACHMENT B

MEMORANDUM OF UNDERSTANDING
FOR THE P-20W STATEWIDE LONGITUDINAL DATA SYSTEM
among

THE NEW JERSEY DEPARTMENT OF EDUCATION
and
THE OFFICE OF THE SECRETARY OF HIGHER EDUCATION,
and
THE NEW JERSEY DEPARTMENT OF LABOR AND WORKFORCE DEVELOPMENT

TIME EXTENSION AMENDMENT

Background and Intent:

This amendment modifies the time period to the existing Memorandum of Understanding (MOU) among the New Jersey Department of Education (NJDOE), The Office of the Secretary of Higher Education (OSHE) and The Department of Labor and Workforce Development (LWD) that expires on June 30, 2017 using the first of five, two-year extensions to establish an agreement to facilitate the exchange, transfer or release of records outlined in the original MOU and provide the governance of such data for the P-20W Statewide Longitudinal Data System (SLDS).

Terms of Agreement:

This amendment, Attachment B to the MOU, extends the term of the MOU until June 30, 2019. All other terms and conditions of the MOU shall continue without change. This amendment does not change the scope of work or funding of the MOU.

Signatures

This extension is effective upon the signature of all of the authorized representatives listed below.

New Jersey Department of Education

Kimberley Harrington, Acting Commissioner of Education — Date: 4/3/17

Evan Linhardt, NJDOE SLDS Representative & Chief Information Technology Officer — Date: 3/29/17

The Offices of the Secretary of Higher Education

Rochelle Hendricks, Secretary of Higher Education — Date 3/27/17

Marie Virella, OSHE SLDS Representative & NJ SLDS State Project Director — Date 3/27/17

The New Jersey Department of Labor and Workforce Development

Aaron Richtner, Acting Commissioner of Labor & Workforce Development — Date 3/27/17

Jeffrey Steller, NJLWD SLDS Representative & Assistant Commissioner of Office of Research and Information — Date 3/27/17

Attachment B

DATA REQUIREMENTS OF NJEEDS

Each Department identified in this document shall, to the extent reasonable available to each Department, provide the data listed below that Department's name/identification. The data requirements specified herein may be amended by any written instrument that manifests the agreement by the impacted Department and Rutgers, The State University of New Jersey. The required Data elements for NJEEDS are as follows:

New Jersey Department of Education

NJ SMART Data System – Annual Transfer

Identifying data elements from NJ SMART:
Sid
First name
Last name
Date of birth

K - 12 Student Demographics:
year of birth
Entering_Race_Ethnicity
race
ethnicity
Entering_Gender
city of residence
zip code
Home Language
Immigrant Status
Entering_Special_Education_Class
Entering_Special_Education_Place
Disability status and type of disability if different from above
Entering_FRPL--Whether student receives free and reduced lunch
Entering_Homeless_Status
Entering_LEP_Program_Status
FPRL_8 -- free and reduced price lunch status in 8th grade

parental education variables

School and district information:
school name -- attending
school code -- attending
district name -- attending

district code -- attending
county name -- attending
county code -- attending
school name -- accountable
school code -- accountable
district name -- accountable
district code -- accountable
county name -- accountable
county code -- accountable

Attendance Information:
First Entry Date Into A US School
Cumulative Days In Membership
Chronic Absenteeism
Cumulative Days Present
Cumulative Days Toward Truancy
Dual Enrollment
dates of enrollment at each school
graduation date
school from which student graduated
School_Exit_Date
School_Exit_Withdrawal_Code

Educational Experience Information:
LEP program start date
LEP program end date
Alternative Education Program
Eighth Technological Literacy
Title I Science
Title I Math
Title I Language
IEP-related data (such as whether student has an IEP, IEP start date, IEP progress, etc.)
Enrolled_in_AP_Bio
Enrolled_in_AP_Calc_AB
Enrolled_in_AP_Calc_BC Enrolled_in_AP_Chem_HS
Enrolled_in_AP_Eng_Lang
Enrolled_in_AP_Eng_Lit
Enrolled_in_AP_Euro_Hist
Enrolled_in_AP_Phys_B
Enrolled_in_AP_US_Gov
Enrolled_in_AP_US_Hist
Enrolled_in_IB_Biology
Enrolled_in_IB_Chemistry
Enrolled_in_IB_History
Enrolled_in_IB_Language_A
Enrolled_in_IB_Math_Stud Enrolled_in_IB_Mathematics

Enrolled_in_IB_Physics
Grades in all of the above
Class rank

Test scores:
LAL_Best_HSPA
LAL_NJ_ASK_3_Scaled_Scores
LAL_NJ_ASK_4_Scaled_Scores
LAL_NJ_ASK_5_Scaled_Scores
LAL_NJ_ASK_6_Scaled_Scores
LAL_NJ_ASK_7_Scaled_Scores
LAL_NJ_ASK_8_Scaled_Scores
Math_Best_HSPA
Math_NJ_ASK_3_Scaled_Scores
Math_NJ_ASK_4_Scaled_Scores
Math_NJ_ASK_5_Scaled_Scores
Math_NJ_ASK_6_Scaled_Scores
Math_NJ_ASK_7_Scaled_Scores
Math_NJ_ASK_8_Scaled_Scores
PSAT_Math
PSAT_Verbal
PSAT_Writing
SAT_Composite
SAT_Critical_Reading
SAT_Math
SAT_Writing

School transfer information
Receiving_County_Code
Receiving_County_Name
Receiving_District_Code
Receiving_District_Name
Receiving_School_Code
Receiving_School_Name
Resident_County_Code
Resident_County_Name
Resident_District_Code
Resident_District_Name
Resident_School_Code
Resident_School_Name
State_ID
Submitting_County_Code
Submitting_County_Name
Submitting_District_Code
Submitting_District_Name

CTE data:
9th grade CTE program status
10th grade CTE program status
11th grade CTE program status
12th grade CTE program status
9th grade CTE CIP
10th grade CTE CIP
11th grade CTE CIP
12th grade CTE CIP

Data Elements from NSC data:
enrolled in state
enrolled out of state
enrolled in 2 or 4 year college
whether institution is public or private
enrolled college name
enrolled college code
enrollment start dates
enrollment end dates
graduation dates
name of college where degree earned
code of college where degree earned

Career and Technical Education Data for Perkins Act Report (NJ Consumer Report Card)

Ssn
First name
Last name
District
Exit date
Cipcode
Exit status
Status

New Jersey Department of Labor and Workforce Development

New Jersey Unemployment Insurance Wage Record Data– to be received quarterly

Social security number
First name
Last name
Wages
Year and quarter the wages were earned
weeks worked in the quarter
employer identification number
Number of employers for which the person worked in the quarter

Industry of employment

Demographics (from AOSOS data) – to be received monthly
Ssn
First name
Last name
Date of birth
sex
year of birth
city
state
zip
county
disability_status_cd
disability_status_name
veteran_status
english_sec_lang_flag
offender_status_flag
edu_max

Services information (from AOSOS data) – to be received monthly
workforce_services_registration_date
workforce_services_termination_date
enrolling_seeker_service_id
exiting_seeker_service_id
ctime
type_of_service_received
service_actual_start_date
service_actual_end_date
service_actual_start_yrq
service_actual_end_yrq
service_obligated_amt
service_completed_successfully_flag
service_cipcode
wia_youth_flag
record_creation_date
fund_allocation_id
fund_id

One-Stop information – to be received monthly
office_id
office_name
Workforce Investment Board number
WIB name

Program participation (from AOSOS data) – to be received monthly

TANF case start date
TANF case close date
GA case start date
GA case close date
SNAP case start date
SNAP case close date

Youth data (from AOSOS data) – to be received monthly
pregnant_parenting_youth_flag
homeless_youth_flag
parenting_youth_flag
school_dropout_flag
in_school_flag

LACES (Adult Literacy Data) – to be received monthly
ssn
first name
last name
date of birth
sex
race
Hispanic ethnicity
highest level of education
whether person was formerly incarcerated -- based on date of release - one record may be kept per student
whether person is homeless
whether person is a veteran
Language Type = Other language proficiency or Correspondence language
whether person has a disability
whether person is a recipient of public assistance
funding stream (NRS or Other)
GED attempt 1 date
score on GED test 1
GED attempt 2 date
score on GED test 2
GED attempt 3 date
score on GED test 3
Literacy level EFL
Intake Date
Date of last hours
Left Date
provider name Agency Name
Agency ID

Vocational Rehabilitation Data (AWARE)

Social security number
First name
Last name
Date of birth
Ethnicity
Race
Sex
Disability Type
Intake Date
Date case approved
Date case closed
Case closure reason
Services received

The New Jersey Office of the Secretary of Higher Education

Data source is the Student Unit Record Data System (SURE)
Transfer Timeframe: Data files for each of the year 2016 through 2020

Also included in the files to be transferred are the routine social security number update files that the institutions submit annually to OSHE.

Identifying data elements from each of these files:
Social security number (PII)

From 12 month enrollment:
Report Starting Date (Y01)
Institution Code (Y02)
Sex (Y04)
Citizenship (Y05)
Student Level (Y07)
Accumulated Grade Point Average (Y08)
Total Credits Attempted (Y09)
Accumulated Native Degree Credits (Y10)
Accumulated Total Degree Credits (Y11)
Hispanic/ Latino Code (Y12)
American Indian/ Alaskan Native Code (Y13)
Asian Code (Y14)
Black/ African American Code (Y15)
Native Hawaiian/ Pacific Islander Code (Y16)
White Code (Y17)

From transfer file:
Reporting Date (T01)
Institution Code (T02)
Class Level (T04)

Program Major (CIP Code) (T05)
Baccalaureate Degree Program (T06)
Transfer Institution Code (T07)
Associate Degree Received (T08)
Degree Credits Accepted by Reporting Institution (T10)
Total Degree Credits Awarded by All Transfer Institutions (T11)
Total Degree Credits Accepted by Reporting Institution (T12)

From Completions:
Date of Award (D01)
Institution Code (D02)
Sex (D04)
Citizenship (D05)
Birth Year (D07)
Admissions Status (D08)
Year of Matriculation (D09A)
Semester of Matriculation (D09B)
Number of Awards Conferred (D10)
Award Type (D11)
Award Major (CIP Code) (D12)
Accumulated Degree Credits (D19)
Accumulated Grade Point Average (D20)
Hispanic/ Latino Code (D21)
American Indian/ Alaskan Native Code (D22)
Asian Code (D23)
Black/ African American Code (D24)
Native Hawaiian/ Pacific Islander Code (D25)
White Code (D26)

From Semesterly Enrollment:
Reporting Date (E01)
Institution Code (E02)
Sex (E04)
Citizenship (E05)
Birth Year (E06)
Zip Code of Home Address at Admission (E07)
State of Residence (E08)
NJ County of Residence (E09)
Registration Status (E10)
Admissions Status (E11)
Matriculation Status (E12)
Attendance Status (E13)
Class Level (E14)
Total Credits Enrolled (E15)

Accumulated Degree Credits (E16)
Accumulated Grade Point Average (E17)
High School Code (E18)
High School Graduation Year (E19)
Program Major (CIP Code) (E21)
Pre-Baccalaureate Degree Program (E22)
Transfer Institution (CEEB Code) (E24)
Computation Remediation Course Enrollment (E28)
Algebra Remediation Course Enrollment (E29)
Reading Remediation Course Enrollment (E30)
Writing Remediation Course Enrollment (E31)
English Remediation Course Enrollment (E32)
Hispanic/ Latino Code (E34)
American Indian/ Alaskan Native Code (E35)
Asian Code (E36)
Black/ African American Code (E37)
Native Hawaiian/ Pacific Islander Code (E38)
White Code (E39)
Dual Enrollment (E40)

Attachment C

The New Jersey Education to Earnings (NJEEDS) Data Safeguard Technical, Security and Confidentiality Infrastructure and Policies

BACKGROUND

The John J. Heldrich Center for Workforce Development ("Heldrich Center") is located in the Edward J. Bloustein School of Planning and Public Policy ("Bloustein School:"), at Rutgers, The State University of New Jersey. Since 1997, the Heldrich Center has emerged as one of the nation's foremost university-based research and policy centers dedicated to finding practical solutions to workforce problems. The Heldrich Center's 20 professional staff and faculty members have considerable years of experience helping national, state and local policymakers, employers, and educators to rethink, restructure, and reform the nation's workforce system to meet the fast-changing demands of a new, more global economy.

The Heldrich Center and its research staff and faculty have extensive knowledge of and expertise in identifying, analyzing, and displaying data from national, state, and local sources on the employment, education, social status, and other demographics (e.g., age, race, gender, etc.) of New Jersey residents. Since 2002, the Heldrich Center has contracted with the NJ Department of Labor and Workforce Development (LWD) to maintain the **Workforce Longitudinal Data System (WLDS)**, obtaining state administrative data files for the WLDS and managing the data in the WLDS to support research and data analyses. In addition, the Heldrich Center has also contracted with the Office of the Secretary of Higher Education (OSHE) to obtain state administrative data files from participating postsecondary institutions in New Jersey, which has allowed the Center, in partnership with these state agencies, to complete longitudinal data system linking college enrollees and graduates (OSHE data) with their labor market outcomes (NJ LWD wage data). In addition, the Heldrich Center has been the recipient of two Workforce Data Quality Initiative (WDQI) grants from the NJ LWD to expand both the data in the WLDS, as well as expand and enhance research and analyses using this data. Under the second WDQI grant and the NJ State Longitudinal Data System (SLDS) federal grant, the state and the Heldrich Center will create the **New Jersey Education to Earnings Data System (NJEEDS)** which will include the existing WLDS data files as well as the following data systems (some data sharing agreements are currently already in place and the data already resides in the WLDS), as well as include driver's license and state identification card data from *the Motor Vehicle Commission (MVC)* as part of the NJEEDS:

NJ Department of Labor and Workforce Development

- New Jersey Unemployment Insurance Wage Record
- New Jersey Unemployment Insurance Compensation Claims/Benefits

- America's One Stop Operating System, including federal WIOA program titles, Wagner-Peyser, Trade Adjustment Assistance Act, and other workforce programs
- Division of Vocational Rehabilitation RSS
- New Jersey Consumer Report Card private training provider

NJ Department of Education

- Perkins Act

NJ Office of the Secretary of Higher Education

- Student Unit Record enrollment data
- Student Unit Record completions data

NJ Department of Human Services

- Supplemental Nutrition Assistance Program (SNAP)

To support these efforts, and the expansion of the WLDS into the NJEEDS which will include NJ Department of Education NJ SMART data and the MVC data as part of the NJEEDS initiative, the Heldrich Center, supported by the Edward J. Bloustein School of Policy and Planning and Rutgers University, reports that it has in place the following technical and infrastructure, and security and confidentiality policies and practices in place.

TECHNICAL INFRASTRUCTURE

The current technical (hardware and software) infrastructure being used by the Heldrich Center and the Bloustein School to support the existing **WLDS** system (and subsequently the development of the NJEEDS) is as follows:

Data Center: The WLDS data and server resides at the Data Center located within the Edward J. Bloustein School of Planning and Public Policy in New Brunswick, NJ. See physical security section below for more details.

Power and Cooling
The Data Center at the Bloustein School is supported by three cooling systems for the purposes of redundancy. All mission critical systems in the Data Center are supported by uninterruptible power supply (UPS) units that can provide emergency power when the input power sources (or main power) fails.

Hardware Platform

1 Dell R720 Server
Dual Xeon 2.70GHz Processors
64GB RAM expandable up to 768GB

Storage Platform
There are six (6) - 300GB internal 15K 2.5" SAS Drives. Ten (10) additional drives can be added internally to the existing chassis with external expansion possible

Data Platform
A custom programmed Java based graphical user interface (GUI) was created for importing and analyzing data sets and is used extensively by the researchers.

Database
Microsoft SQL Server

Network
10 Gb Collapsed backbone network with Cisco Switches at both the access and aggregation layers.

Router
Juniper QFX5100

Secure File Transfer (SFTP)
Bitvise SSH Server

SECURITY STANDARDS

Data Transmission: The Heldrich Center only transmits or exchanges State of New Jersey or other parties' data through a written data sharing agreement. Approval to use this data for research must be requested in writing. Research may be conducted only when expressly permitted by the data owner. The Heldrich Center only transits or exchanges data with the State of New Jersey (or other parties) through secure means supported by current technologies. All data defined as personally identifiable or confidential by the State of New Jersey and Rutgers University or applicable law, regulation or standard is encrypted during any transmission or exchange of that data.

a. Uploads
   Data sets are transmitted securely using SFTP to the server from a dedicated and standalone computer workstation that only exists for the purposes of obtaining data files from external agencies and uploading them to the server. This system is normally off line, but when it is used, it can only access the specific sites that provide the data for the researchers. The system is also locked down using a program that does not allow any permanent changes to be made to the system.

b. Downloads
   Downloading data and providing it to external agencies requires coordination with the

Bloustein School's Information Technology Services Office. The data is moved physically to an SFTP server that is kept off line except when needed for transferring data to external agencies. The external agencies are given access to the data and then the data is securely deleted and the system is taken off line.

c.

Physical, Network and Security: The Heldrich Center, through the Bloustein School and Rutgers University, maintains physical, system/network and workstation security that includes the following:

a. Physical Security

The **WLDS/NJEEDS** server is physically stored in a rack in a physically secure data center located within the Bloustein School building. This facility has redundant climate control systems, UPS protection, and is protected by card swipe access. The card swipe programming is managed by the Rutgers Campus Safety Office. In addition, the server itself is headless and is not identified in any way within the data center.

b. Network System Security

1. Network System Users

In addition to compliance with the Bloustein School NPPI policy, alerts related to SPAM and phishing attempts are sent out regularly by the Bloustein School Information Technology Services Office who also performs internal phishing expeditions to find vulnerable users within the environment. Anyone who falls victim to internal phishing expeditions is sent information to improve their security awareness and they are offered in person training related to phishing.

2. Computer Workstations

Work stations within the Bloustein School and Heldrich Center are secured using hardened baseline images, multiple endpoint security programs (Symantec Endpoint Protection and Malwarebytes) with console based monitoring solutions along with limited rights policies that prevent end users from making changes on the systems. These systems are also scanned regularly for sensitive data to ensure that secure data is not being saved locally. This scanning is currently being upgraded to an agent based solution to improve Data Loss Prevention efforts.

3. Dedicated Secure Server

The dedicated server being used for the **WLDS/NJEEDS** has been configured with only the necessary services installed to reduce the attack surface. The system has restrictions in place that only allow identified research workstations at the Heldrich Center to access the system. In addition, the server requires complex passwords and does not have any direct Internet access.

4. Network Segmentation
   The Heldrich Center research workstations that have access to the secure **WLDS/NJEEDS** data are segmented on their own network, which only has services enabled that are required for the users who are authorized to conduct work and who have complied with the Bloustein School and Heldrich Center data security and confidentiality policies and protocols. This network segment is monitored closely by the Bloustein Information Technology Services Office and Rutgers University Office of Information Technology for anomalies in traffic and any other suspicious behavior.

5. Firewalls
   Rutgers University has a perimeter level firewall that protects internal networks and a centralized networking office also runs security tools on network traffic to help identify and report malicious behavior on the Rutgers network. The Bloustein School uses a Next Generation Firewall to help protect our internal networks and that separates the Bloustein School from the larger Rutgers University environment. The **WLDS/NJEEDS** server used by the Heldrich Center sits behind yet another (second) firewall restricting access to only the systems used by the researchers

6. Monitoring Dashboards
   The Bloustein School also uses a tool to aggregate console and server log data and to create dashboards for monitoring the environment.

7. Incident Response
   A security incident can be declared by any one of the Information Technology Services Office staff at the Bloustein School based on a monitoring alert from either the Rutgers University Network Operations Center, which runs Stealthwatch on campus networks, or from a monitoring alert generated from the Nexgen firewall, Symantec Endpoint Protection Console, Malwarebytes Console, or the Splunk dashboard tool. In addition, an incident can be declared based on a report from one of the research staff. Incident response then follows internal procedures for the steps of containment, eradication, and recovery.

8. Breach Identification and Reporting
   If a breach has been discovered, the incident is reported to the Rutgers Information Protection Services Office who will perform an investigation using forensics to create a report that is sent to a review board, which determines the extent of the breach and makes a decision regarding notification. The breach will also reported to the Data Owners as required in the corresponding Memorandum of Agreement.

d. System Data Security

1. Data Storage and Backups
   The **WLDS/NJEEDS** data on the dedicated server is stored in an encrypted volume using 256 bit AES encryption that requires the use of an additional password to open the data. Backups for the data are performed weekly and the backups are stored on a locally attached storage device that also uses a 256 bit AES encrypted volume and is only opened for the backup and this is dismounted.

2. Data Disposal
   All hard drives used within the environment are sanitized using NIST SP 800-88 media erasure guidelines prior to disposal. In addition, drives that are used in conjunction with sensitive data research go through physical measures to ensure that the data is not accessible.

3. Administrative and Personnel Security
   Rutgers University, the Bloustein School, and the Heldrich Center have developed, as well as maintain, monitor and enforce security responsibilities required for data owned by the State of New Jersey. Policies and protocols evident in policies, practices and protocols articulated earlier in this document, include responsibilities for administration and management of the technical infrastructure, implementing, maintaining and enforcing security and the protection of confidential data, as well as policies and protocols for maintaining and enforcing the integrity, storage and access to the data

DATA CONFIDENTIALITY POLICIES AND PROCEDURES

All personally-identified data supplied by the State of New Jersey are considered confidential. The Heldrich Center and the Bloustein School secure all data from manipulation, sabotage, theft and/or breach of confidentiality through the use of policies and practices designed to provide the utmost protection, security and safety of the data.

As required by Rutgers, The State University of New Jersey, the Bloustein School has a school policy to safeguard non-public personal information (NPPI), which includes data provided by the State of New Jersey in the **WLDS/ NJEEDS**. The intent of this policy is to minimize the possibility of access or the manipulation of sensitive information by unauthorized individuals or organizations. The school has a set of guidelines related to the storage, usage, transportation, and transmission of electronic and hardcopy sensitive information. It also requires that any employee (or student) who is using sensitive data identify themselves as "data custodians" within the Bloustein School. Adherence to these policies by the members of the Edward J. Bloustein School of Planning and Public Policy community ensures the confidentiality and integrity of sensitive information, while also making this information available to the individuals who may need to use it for administrative, instructional, or research-related functions.

Rutgers classifies data through the level of risk involved related to various forms of data; these classifications are:

Restricted Data (highest level of sensitive)

Restricted Data is the most sensitive information and requires the highest level of protection. This information is usually described as "non-public personal information (NPPI)" and is related to people or critical business, academic or research operations under the purview of the Owner/Data Custodian. Restricted data includes, but is not limited to, data that Rutgers is required to protect under regulatory or legal requirements. Unauthorized disclosure or inappropriate use of restricted information could result in adverse legal, financial or reputational impact upon the university, as well as individuals and organizations. Examples of Restricted Data include but are not limited to: sensitive student or employee identifiable information (i.e., Social Security Number, driver's license number, etc.), credit card information, confidential research, and file encryption keys, as well as certain financial records, medical records, legal records, student records, police records. Data provided by the State of New Jersey to the Heldrich Center in the **WLDS**/ **NJEEDS** fall under the category of restricted data with the highest level of sensitivity.

Limited Access Data

Limited Access Data is information that does not meet the requirements of restricted data but requires a moderate level of sensitivity and protection from risk and disclosure. Limited Access Data is the default and should be used for data intended for use within the University or within a specific workgroup, department or group of individuals with a legitimate need-to-know. Limited Access Data may be information one unit decides to share with another outside their administrative control for the purpose of collaboration. Unauthorized disclosure or inappropriate use of Limited Access Data could adversely impact the university, individuals, or affiliates but would not necessarily violate existing laws or regulations. Examples of Limited Access Data include but are not limited to: incomplete or unpublished research, internal memos or reports, personal cell phone numbers, project data, data covered by non-disclosure agreements. Although most Limited Access data is not technically NPPI, Rutgers University protects it in the same manner in order to comply with the security requirements of organizations providing data as part of grant requests.

Public Data (low level of sensitivity)

Public data is information that may or must be open to the general public. It is information with no existing local, national or international legal restrictions on access or usage. Public data, while subject to University disclosure rules, is available to all individuals and entities both internal and external to the University. While the requirements for protection of public data are less than that of Restricted and Limited Access Data, sufficient controls are maintained to protect data integrity and unauthorized modification or destruction. Examples of Public Data include but are not limited to: data on websites intended for the general public, course listings, press releases, marketing brochures, university maps, and annual reports.

Data Custodian

A data custodian is anyone who has access to, stores, transmits, or uses NPPI at the Edward J. Bloustein School of Planning and Public Policy (this includes the Heldrich Center). This includes restricted data and limited access data that is being protected as restricted data for the purposes of grant requests or in order to provide better protection on that data.
Source: http://rusecure.rutgers.edu/content/draft-information-security-classification-policy

Members of the Edward J. Bloustein School of Planning and Public Policy community are required to know what constitutes NPPI. In addition, if an individual meets the criteria for being deemed a data custodian, that individual must:

- Register as a data custodian with the Bloustein School by completing the form that accompanies the NPPI policy and submitting it to the Information Technology Services office. All registered data custodians are included in a database for tracking sensitive information usage at the Bloustein School. Anyone who meets the criteria of a data custodian whether an employee, student, or affiliate member must register immediately upon becoming a data custodian.

- Maintain NPPI in a dedicated, centralized, and secured location. Data custodians are required to maintain the following procedures and protocols in the storage of data:

    - Electronic information only resides on dedicated file servers (networked drives) within the Edward J. Bloustein School of Planning and Public Policy environment.

    - Hard copy information are stored in locked drawers or filing cabinets when not being used. When such sensitive information is being used, the material is not be left unattended, nor should any such information be left in a room that is unlocked. The information may not be left outside of its primary storage location overnight.

- Not store electronic NPPI on local systems, portable systems, portable devices, or systems being used for remote access to the Edward J. Bloustein School of Planning and Public Policy networks.

- Not store or transfer NPPI using university or personal email accounts.

- Not transport hard copy NPPI outside the confines of the school or center in which it is being held.

- Not publish NPPI to web sites or any internal or external file sharing systems other than the dedicated Edward J. Bloustein School of Planning and Public Policy file sharing servers. This includes files sharing systems like drop box and replication systems like iCloud.

- Not take any NPPI should an individual no longer be employed by, or no longer be associated with the Bloustein School.
- Appropriately discard unused/unnecessary NPPI as soon as possible by complying with the procedures outlined below under "Secure Removal and Disposal of NPPI.".
- Notify the Bloustein School's Information Technology Services or the Business Services Office immediately if there are any possible threats related to the compromise of NPPI. This includes any security threats to computer systems using NPPI. For hardcopy information, this includes any possible breach of physical security to the locations where NPPI stored.
- Not remotely access NPPI on the secure servers at the Bloustein School through a VPN connection if they have any suspicion that the machine being used to connect to the information is infected with malware, spyware, or a computer virus.

Data Custodian at the Bloustein School and Heldrich Center - User Responsibilities

Data custodians are responsible for storing all sensitive information on the designated systems within the technical environment of the Edward J. Bloustein School of Planning and Public Policy. The protection of these systems and the associated internal networks are the responsibility of the Information Technology Services staff of the Edward J. Bloustein School of Planning and Public Policy. If an individual is using sensitive information based on an exception request, then that individual is responsible for the safety and security of that data. Data custodians are expected to notify Information Technology Services or the Business Services Office immediately if any threats arise that may jeopardize the security of NPPI. It is also expected that any individuals acting under an exception request will adhere to any additional security related procedures recommended by the technical and business staff of Bloustein Dean's office.

Proactive Restricted Data Discovery Processes

The Information Technology Services unit of the Edward J. Bloustein School of Planning and Public Policy uses scanning tools to proactively try to identify Restricted Data that resides on systems within the organization to ensure that it is adequately protected. These scanning tools are used on a regular basis and any restricted data that is discovered will result in communications with the owner of the data to ensure that the data should be stored in its current location, that it is adequately protected, and to ensure that the individual is properly registered as a data custodian. Similarly, the Bloustein School's Business Services Office periodically conducts in-person audits for hardcopy restricted data.

Secure Removal and Disposal of NPPI

Any system that houses NPPI requires special attention prior to its disposal. Specifically, NPPI must be securely removed so that there are no traces of that data left on the existing system or device. When such a device needs to be disposed of, the Information Technology Services staff at the Edward J. Bloustein School of Planning and Public Policy must be contacted to provide

assistance with securely deleting such information through drive sanitization processes. This includes computers, copiers, fax machines, and portable storage devices.

Sensitive information in hardcopy form must be destroyed once it is no longer deemed necessary by school wide and university wide records retention policies. Hardcopy sensitive information must be cross shredded prior to disposal. Unnecessary NPPI must remain in a locked filing cabinet or desk until it is shredded. In addition, any credit card information recorded for the purposes of processing a transaction must be destroyed immediately after completing the transaction.

Security Training

All members of the Edward J. Bloustein School of Planning and Public Policy are required to complete an online information security awareness training session and take a quiz associated with that training. If an individual scores below 85 percent in the training, an in-person training session is required. In addition, individuals are required to take this training at the beginning of their employment with the school and at least once every three years thereafter. These training requirements are also applicable to any registered data custodian whether he or she is part of the school or not.

Policy Modifications or Updates

NPPI security and confidentiality policies are reviewed and modified or updated as necessary or if any major security issues arise related to the use of NPPI.

Enhanced Practices Engaged by the Heldrich Center

In addition to knowledge and adherence of the Bloustein School policies noted above, employees at the Heldrich Center, who are responsible for working with confidential data, must also:

- Read and acknowledge receipt and review of the Rutgers University Office of Information Technology Acceptable Use policy;

- Sign a confidentiality and non-disclosure agreement that they will not disclose any confidential wage record information to anyone either inside or outside the university who is not authorized to have access to that information;

- Receive and acknowledge receipt and review of the most up-to-date version of the *Wage Record Interchange System (WRIS) Standards and Guidelines for the Handling of Confidential WRIS Data*;

- Sign the WRIS acknowledgement indicating that they understand the confidential nature of wage data and the guidelines for handling wage record data that are laid out in the *Standards* document;

- Receive detailed verbal instructions and in-person training regarding the security and confidentiality requirements of all State of New Jersey (and other parties) confidential data, how it must be stored only on the secure server; that it may never be stored on a desktop

computer or any other portable or mobile device; and that all work using this data will be conducted remotely using the secure server.; and

- Receive the latest version of the Bloustein School NPPI policy and sign the Bloustein School's NPPI Policy, initialing next to each element of the policy to indicate their understanding and intent to comply with each element (for those employees handling sensitive data);

- After receiving detailed verbal instructions with respect to confidential data being stored only on a secure server, all employees will be asked to sign a form acknowledging having been so briefed and stating their intention to comply, and be advised of disciplinary action that may occur if this operating protocol is violated; and

- Require all research and evaluation unit staff to participate on a mandatory basis in expanded internet and security training including being informed of such information as found at http://technology.msb.edu/helptopics/security/security.htm#1.

In addition, Heldrich Center employees working on data analysis using data governed by negotiated and established data sharing agreements with external parties are advised of the specific legal, regulatory and other standard provisions of the specific negotiated agreement including the provisions requiring the Heldrich Center to instruct all personnel having access to the disclosed data with regard to confidentiality. Personnel are required to review and sign an "Acknowledgement of Responsibilities for Maintaining Data Confidentiality".