Ohio Board of Regents
Higher Education Information System (HEI)

HEI DATA ACCESS AND SECURITY POLICY
Revised November 5, 2012

Section 1: Purpose

The Higher Education Information (HEI) system is a comprehensive relational data warehouse at the Ohio Board of Regents that contains data supplied by Ohio's colleges and universities via the use of the Internet. HEI also contains data supplied by several other federal, state, and local entities. This document outlines the policies and procedures that are in place at HEI to ensure the security and privacy of HEI data.

HEI staff will monitor these policies and communicate changes as events or technology warrant. For questions, please contact the HEI help desk at help_hei@regents.state.oh.us.

Section 2: Definitions

A. Confidentiality means how personally identifiable information collected by an authorized agency is protected and when consent by the individual is required.

B. Directory information means information contained in an education record which would not generally be considered harmful or an invasion of privacy if disclosed. It includes, but is not limited to, the student's date and place of birth, field of study, dates of attendance, degrees and awards received.

C. Education records means those records directly related to a student and maintained by an educational agency or institution.

D. Family Educational Rights and Privacy Act (FERPA) means the federal law codified at 20 U.S.C. 1232g and its implementing regulations found in Title 34 C.F.R. Part 99. A description and additional information can be found at: http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

E. Legitimate educational interest, for purposes of this policy, is an endeavor that furthers the understanding of educational practices, methods, and/or theory through formal, accepted research practice.

F. Personally identifiable information means information contained in an education record such as a personal identifier, characteristic, or other information that would make a student's identity easily traceable.

G. Privacy means the right of an individual to have personal information adequately protected to avoid the potential for substantial harm, embarrassment, inconvenience, or unfairness.

H. Research means a formal investigation designed to develop or contribute to general knowledge.

Section 3: Data Security

A. Security includes the measures in place to ensure that records are not lost, stolen, vandalized, illegally accessed, or otherwise rendered useless. Since the data are stored on computers, it is essential that there be a high level of protection that provides integrity and availability commensurate with the level of risk and magnitude of harm.

B. HEI data are maintained on a secure computer system and archived daily. Archived information is stored in a fire-proof off-site location. The procedures used to ensure the privacy and security of computer records include but are not limited to: password applications that restrict access to data elements and files only to those with authorization, frequent password changes to guard against break-ins, the use of encryption, and monitoring of user access to the secured files.

C. All external connections to the agency's restricted data are controlled and restricted by a State of Ohio Department of Administrative Services firewall and a secure web server implementing Secure Socket Layer (SSL) technology. Communication with agency servers is encrypted and requires username and password authentication.

D. HEI will enforce security of computer systems through appropriate hardware/software, systems, authorizations, and practices required to ensure the confidentiality of computing systems and data. Users must not violate confidentiality of data by sharing files or information with unauthorized individuals or provide access to confidential data to unauthorized individuals.

E. The Social Security Numbers (SSNs) are the primary unique identifier for student data in HEI and are collected from Ohio colleges and universities for the evaluation of state assisted programs in accordance with FERPA. The SSNs are converted into unique OBR identification numbers and given additional security in the information system.

Section 4: Data Access

Most data in HEI are publicly accessible through electronic reports and queries located on the HEI web page at http://www.ohiohighered.org/hei. Additional data are considered by the Regents to be restricted, and may not be accessed without authorization by campus liaisons and the HEI Director. The procedures discussed in this section refer to access to "restricted" data.

A. Campus liaisons issue user accounts and determine user access levels in the restricted areas of HEI. Restricted access allows an authorized user, with a legitimate educational interest, the opportunity to select and retrieve special information from the HEI system. Users with access to restricted queries can retrieve aggregate data on any state assisted institution. The data obtained through restricted queries can be considered, in certain cases, sensitive and subject to misinterpretation or contextual explanation. In addition, data retrieved from restricted queries for terms which have yet to be used in subsidy calculations are subject to change as campuses and the Regents review these data during the subsidy development process. For these reasons, persons authorized to have access to restricted data should be thoroughly familiar with the data elements, timing of campus data submissions and subsidy calculations, data limitations, and their responsibilities regarding data dissemination noted below.

B. Restricted data containing personally identifiable student information can only be accessed and retrieved by authorized users at the institution(s) from which the student was enrolled. The responsibility regarding privacy and the appropriate use of these restricted HEI data rests with the authorized user and their employing institutions. An authorized user must adhere to their institution's policy under Family Educational and Rights and Privacy Act of 1974 (FERPA), as well as, any other institutional procedures pertaining to the security and confidentiality of student information.

C. Security and confidentiality of restricted HEI data is a matter of concern by the Regents. The Regents controls access to HEI restricted data areas. A Request for Access to Restricted Data Authorization Form must be signed and completed for any campus user or Regents approved user who is to have access to restricted data areas. Specific instructions are located on the authorization form. Each request for access is individually evaluated by the Regents and it is expected that only those persons identified on request forms will have access to restricted HEI data. Access is issued to a person, not a position or work station. Approval for access will be evaluated based upon a "legitimate educational interest" or demonstrated "need to know" the information as determined by the campus liaison and/or the Regents. The Regents reserves the right to deny access to any such application for access to restricted HEI data.

Section 5: Disclosure of Data

A. In accordance with Family Educational and Rights and Privacy Act of 1974 (FERPA), disclosure of personally identifiable information in HEI to the public is not allowed without prior written consent of the institution(s) and person(s) involved. In the event that consent is provided, the Regents will note the names of the parties who received the information and an explanation of the legitimate educational interest under which the information was disclosed.

B. HEI only provides aggregate data to the public in published reports or in response to ad-hoc requests. In planning and producing analyses and tabulations, the general rule is that there should be no cell (or category) published in which there are fewer than five respondents, or in which personal information could be obtained by subtraction or other simple mathematical manipulations. In these cases an asterisk (*) should be inserted in the cell.

C. Private or confidential data will be released as stated in federal regulation 34 C.F.R. Part 99 to authorized staff of the postsecondary education institutions who have released the data to HEI and only when the determination has been made that there are legitimate educational interests, under federal regulation 34 C.F.R. Part 99.36(b)(2).

D. HEI restricted query data should be used for evaluative and planning purposes within an institution, rather than dissemination beyond a campus or used to as method to contact students. In such limited cases where HEI restricted query data are disseminated to public settings, the Regents suggest a policy of *responsible data dissemination*. This policy includes:

- Removal of any personally identifiable information, including aggregate data that may personally identify an individual.
- Acknowledgement at all times of relevant data anomalies which have been noted by HEI staff and institutions.
- Appropriate notice to the Regents and Chief Executive of any affected institutions that restricted HEI data are to be disseminated (or in a less desirable instance have been disseminated) in a public setting with timely opportunity for campus review of such data.
- Maintenance of any query code (called SQL) used to generate an HEI restricted data outputs. This is necessary to allow external verification of the validity of query code in presenting and interpreting findings.

E. To encourage responsible data dissemination, the Regents reserve the right to maintain in a publicly accessible location the identification of all individuals authorized to engage in restricted query access. Further, the Regents reserve the right to maintain an internal logging of queries of HEI restricted data by authorized users.

F. The Regents will provide a current web site for any known campus data anomalies that may be retrieved by restricted data queries and reports. Users are responsible for routine reviews of this web site and being aware of data anomalies that may impact analysis of restricted data.

G. Any data sharing agreements between the Regents and other agencies or organizations will be established without compromising the confidentiality of individuals. If a data set containing personally identifiable information is released across agencies or to outside organizations the following conditions must be met:

- A written explanation of the legitimate educational interest for data sharing

- The data are used solely for the purpose requested
- Appropriate agreements must be signed by all parties to ensure compliance with FERPA
- All records will remain private and destroyed when no longer needed
- The party to whom the data are released does not disclose the information to any third party
- Penalties for inappropriate records use or re-release of records must be stated clearly in the agreement.
- The data are protected in a manner that does not permit the personal identification of an individual.

Section 6: Campus User Responsibilities

A. A person granted restricted access must sign the appropriate **Request for Access to Restricted Data Authorization Form** acknowledging an understanding of the person's responsibilities for password security and maintaining the confidentiality of the data that he/she accesses. This signed agreement must be kept on file by the campus liaison and Regents.

B. A person granted restricted access is responsible for security of his/her password and protection of information. At no time should any individual share his/her password with another person, display the password in public view, or install the password for a group account. Each person approved for access is responsible for signing off when finished with access.

C. A person granted restricted access must adhere to their institution's policy under Family Educational and Rights and Privacy Act of 1974 (FERPA), as well as any other institutional procedures pertaining to the security and confidentiality of student information. In addition, a person with access should be aware that the penalties for violation of FERPA can be the withdrawal of federal funds from the institution, as well as criminal and/or civil sanctions.

D. All persons accessing restricted data must guarantee to maintain data about individual students in a secure fashion, such that it cannot be viewed by unauthorized individuals by screen, file access, or in printed form. Any personally identifiable confidential data contained in print form or on computer files which are no longer needed should be destroyed in such a way that identification of a student is not possible. **Also see "Section 5: Disclosure of Data" above.**

E. Users understand that access to HEI is a privilege not a right and that violations of this policy or its procedures can result in the termination of this privilege and/or disciplinary measures which include legal remedies if required.

F. If an employee terminates employment with the institution or transfers within the institution, the Campus Liaison must notify the Regents in order to initiate access deletion. A **Request for Access to Restricted Data Authorization Form** must be submitted to the Regents for a personnel replacement.

G. If a security violation is detected the user should immediately change their password and notify the Campus Liaison or the HEI help desk if appropriate. The Campus Liaison is responsible for contacting the Regents when a password security violation has been detected.

Section 7: OBR Employee User responsibilities

A. A person granted restricted access must sign the appropriate **Request for Access to Restricted Data Authorization Form** acknowledging an understanding of the person's responsibilities for password security and maintaining the confidentiality of the data that he/she accesses. This signed agreement must be kept on file by the OBR Supervisor and HEI Director.

B. A person granted restricted access is responsible for security of his/her password and protection of information. At no time should any individual share his/her password with another person, display the password in public view, or install the password for a group account. Each person approved for access is responsible for signing off when finished with access.

C. A person granted restricted access must adhere to the Family Educational and Rights and Privacy Act of 1974 (FERPA), federal law codified at 20 U.S.C. 1232g and its implementing regulations found in Title 34 C.F.R. Part 99. In addition a person must abide by any agency policies and any state laws pertaining to the security and confidentiality of personal information. In addition, a person with access should be aware that the penalties for violation of FERPA can include criminal and/or civil sanctions.

D. All persons accessing restricted data must guarantee to maintain data about individual students in a secure fashion, such that it cannot be viewed by unauthorized individuals by screen, file access, or in printed form. Any personally identifiable confidential data contained in print form or on computer files which are no longer needed should be destroyed in such a way that identification of a student is not possible. **Also see "Section 5: Disclosure of Data" above.** Sending personally identifiable information (e.g. SSN's) via email to campus data reporters is strictly prohibited. OBR has a secure website that will allow an employee to send and receive files containing personally identifiable information to and from campus data reporters in a secure manner**.**

E. A person granted internal restricted access must guarantee to maintain data about the technical infrastructure of HEI in a secure fashion, such that database, table, and server

configurations cannot be viewed by external individuals by screen, file access, or in printed form.

F. Users understand that access to HEI is a privilege not a right and that violations of this policy or its procedures can result in the termination of this privilege and/or disciplinary measures which include legal remedies if required.

G. If an employee terminates employment with OBR or transfers within the agency where restricted access is no longer part of their duties of employment, the supervisor must notify the HEI Director in order to initiate access deletion. A **Request for Access to Restricted Data Authorization Form** must be submitted to the HEI Director for a personnel replacement.

H. If a security violation is detected the user should immediately change their password and notify the HEI help desk if appropriate.