PASSPORT DATA MANAGEMENT PLAN

February 2016

The Interstate Passport

The Passport Tracking System, Central Data Repository, and annual institution-level reporting make data from the Interstate Passport usable for longitudinal analysis and outcomes measurement. Data Management is integral to the success and scalability of the initiative. This Plan details data management, descriptions, sharing, privacy, security and rights.

Passport Data Management Plan

Table of Contents

OVERVIEW

The Interstate Passport is a grass-roots project, conceived by the chief academic leaders in the WICHE region, to develop a new framework for block transfer of lower-division general education based on learning outcomes and transfer-level proficiency criteria. Students who earn a Passport at one participating institution and transfer to another Passport school have their learning achievement recognized in its entirety; they are not required to take any courses in the receiving institution's Passport block to meet lower-division general education requirements. The ultimate goal of this initiative is to increase the percentage of students successfully earning degrees by lowering one of the potential barriers to completion.

One measure of the success of the initiative is to demonstrate that students who earn a Passport and transfer to a Passport institution complete college at a higher rate than students who do not earn a Passport. Because college completion measures typically involve a large lag (as much as four to six years or more for a bachelor's degree), intermediate measures and data collection are important components of the initiative. The Passport Tracking System addresses the need for intermediate and long-term measures. Each Passport signatory institution agrees to supply data annually on the Passports it awards. Each institution also agrees to send data about the academic progress of students who transferred into its institution (those with Passports and those without) for two terms after they transfer.

Data Management for the initiative has two distinct phases. In Phase I, Passport Learning Outcomes and proficiency criteria were developed for only three foundational skill areas: oral communication, written communication, and quantitative literacy. Sixteen institutions involved in the initial agreement of this pilot phase began awarding the Passport Phase I to students for achievement in these three skill areas. The institutions submitted data reported directly to the Passport's Central Data Repository (CDR), located at Utah State University. In the initial phase of data management, only aggregate data—primarily averages, sums and counts—is supplied. This reporting is in the form of an Excel template that is completed by each institution and then emailed to the CDR annually. The CDR verifies and organizes the data and provides reports back to each Passport sending institution about its students for use in continuous improvement processes. Because receiving institutions have agreed to supply data about transfer students from other Passport institutions, it is possible for Passport sending institutions to know if their Passport students have better academic progress, on average, compared to students who transferred without a Passport. It is anticipated that better academic progress will translate to an increased percentage of students earning a degree. In addition to customized institution-level reporting, the CDR also provides a set of aggregate reports annually to the Passport Review Board (PRB) for evaluating the overall effectiveness of the Passport .

As part of Phase II of initiative, development of the framework was completed. Passport Learning Outcomes and proficiency criteria were developed in the remaining six knowledge and skill areas: natural sciences, human cultures, creative expression, human society and the individual, critical thinking, and teamwork and value systems. During this phase the Data Management Plan involves a change in institutional reporting. The Phase I data management plan was based on a relatively small number of institutions (16), and a desire for simplified data collection and a low barrier for entry and data management (Excel templates, aggregate data reporting only). Phase II of the data management plan addresses the needs of the project to go to scale: managing a much larger volume of student-level data while safeguarding privacy and ensuring the security of data involved in the initiative.

In Phase II, institutions will leverage the data infrastructure, system management and controls of the National Student Clearinghouse (Clearinghouse or NSC)—the nation's leading provider of educational reporting, data exchange, verification, and research services. Data reporting is simplified by leveraging NSC's existing

reporting infrastructure, formats and data elements. More than 3,600 colleges and universities participate in the Clearinghouse, reporting enrollment and degree information regularly throughout the year. Data security and privacy are enhanced because of NSC's robust investments in and commitment to student privacy and data security (http://www.studentclearinghouse.org/about/privacy_commitment.php). During NSC's almost 20-year history, the confidentiality and privacy of [now] more than 100 million student records entrusted to the 501(c)(6) nonprofit have been maintained without a breach of security. Full details of NSC's security and privacy infrastructure can be found in Appendix A: *NSC Security Program Overview V1.1*

The pilot phase of the Passport, funded by the Carnegie Corporation of New York, was completed in spring 2014. Those institutions that signed the Passport Network Memorandum of Agreement submitted data to the CDR for the first time in November 2014, and received institution-level reporting of results in March 2015. Institution-level reporting by the 17 institutions currently participating, for the 2014-2015 academic year, is being collected by the CDR (November/December 2015). Results will be provided to institutions and the Passport Review Board at the end of January 2016. By the end of calendar year 2016, institutions will switch over to NSC reporting (for the 2015-2016 AY) and Phase II of the Data Management Plan will be fully in effect. Funding provided by the Bill & Melinda Gates Foundation and Lumina Foundation overlaps both data management phases, and this document provides details for both Phase I – currently in effect – and Phase II data management – currently under development with the Clearinghouse, project staff, participating registrars and institutional researchers, and key stakeholders including the PRB.

CORE PRINCIPLES FOR PASSPORT DATA MANAGEMENT

1. The Interstate Passport Network (Network) is committed to safeguarding individual privacy and ensuring the security of all data collected in the initiative, while providing for the necessary sharing of data that enables institutions and key stakeholders to evaluate outcomes of the Initiative.
2. WICHE staff, participating institutions, sub-contractors and any other participating entities must, at a minimum, comply with all relevant federal and state laws and regulations with regard to privacy and data security, including but not limited to the Family Education Rights and Privacy Act ("FERPA").
3. The Interstate Passport Network will clearly establish binding policies for data ownership and use, including relevant intellectual property, for all parties to the initiative.
4. All personally identifiable information provided by institutions to the NSC for the Passport program will remain at all times the property of that individual institution and remains the legal responsibility of the institution disclosing the data. Such data may be used by WICHE and its authorized sub-contractors only for the purposes set out in the Passport Agreements. WICHE and its sub-contractors are prohibited from selling the data received under such agreements or using institution-specific data for any
5. Institutions providing data to the initiative shall have a role in determining the limitations on access to and the use of data they provide through representation on the Passport Review Board and the Passport State Facilitators working group.
6. For the purposes of the Passport Initiative, WICHE is serving as a School Official of multiple institutions of higher education. WICHE designates Utah State University (the CDR) and NSC as sub-contractors working under its direction and control to perform services for the participating Passport Institutions and WICHE related to facilitating student transfer among institutions through the Passport

and to perform certain research and data aggregation services to measure the medium and long-term impact of, and to improve, the Passport program.

7. The National Student Clearinghouse is authorized by WICHE as a "School Official" of the participating Passport institutions to create aggregate, de-identified reports required to measure the impact of, and to improve, the Passport program. Such reports become the property of WICHE upon delivery as a Work for Hire under the U.S. Copyright Act. NSC will be given appropriate credit as a data source on any reports that are published publicly.
8. Authorized sub-contractors, including Utah State University and the National Student Clearinghouse, may utilize certain proprietary technology to perform services contracted under the Passport Initiative. All such technology, including software or business processes or other technology shall remain at all times the property of the sub-contractor and neither WICHE nor the participating institutions will acquire any right, title or interest therein.

DEFINITIONS

"FERPA" stands for the Family Educational Rights and Privacy Act of 1974 (codified at 20 U.S. C. 1232g) and associated implementing regulations, as they may be amended from time to time. The regulations issued by the U.S. Department of Education are available at http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

"Personally identifiable information" means any information defined as personally identifiable information under FERPA or relevant state law.

"De-identified" indicates data or information that has been subjected to a disclosure limitation method, or methods, to prevent unauthorized release of information about individual students, in accordance with the guidelines provided by Privacy Technical Assistance Center (PTAC) of the U.S. Department of Education: http://ptac.ed.gov/sites/default/files/data_deidentification_terms.pdf.

"Aggregate data" are de-identified data presented in a form such that no individual student details are presented or can be discerned. Data blurring is a disclosure limitation method used in the creation of Passport aggregate data to prevent unauthorized release of student information. Aggregate Passport results are presented as counts, averages, and sums.

PHASE I

INTERSTATE PASSPORT DATA DESCRIPTION

With Phase I of the Interstate Passport fully operational and Phase II under development, it is worth revisiting the data being collected and reported by current participants, and providing clear definitions for the data elements currently used for reporting and outcomes management. Each Passport signatory institution supplies aggregate data, annually, to the Passport Central Data Repository. The following de-identified measures relevant to the initiative are reported:

- Total number of Passports awarded each term, and the mean number of credits earned when the Passports were awarded
- Average academic progress – the total number of credits earned at each grade level (A, B, C, etc.) – for all students transferring into the institution, with and without a Passport, for the first two terms after transfer in the specified timeframe
- Average academic progress for "native" students for two terms, after earning a Passport

For the purposes of Interstate Passport reporting, the following definitions hold:

Native Students	=	Students attending the reporting institution who are not transfers
Transfer Students	=	Students transferring into the reporting institution
Passport Students	=	Students who have earned a Passport
Non-Passport Students	=	Students who have not earned a Passport
Passport Institution	=	Institution that is a signatory to the Passport initiative

Passport signatory institutions provide the CDR with aggregate data for four categories of students. All students being reported must fit into one of these four groups:

- All "native" Passport students at the reporting institution
- All non-Passport transfer students at the reporting institution
- All transfer students that have earned a Passport and are attending the reporting institution – organized and aggregated by the name (code) of the institution where they earned their Passport
- All non-Passport transfer students who are attending the reporting institution – organized and aggregated by the name (code) of the Passport institution that they *transferred from*, with all transfer students from non-Passport Institutions aggregated into a single "TRANS" category.

For a list of participating Passport institutions and the data elements, please see Appendix B: *Passport Signatory Institutions and Passport Extract Fields.*

DATA ACQUISITION, INTEGRITY AND QUALITY

Each Passport signatory institution signs a Memorandum of Understanding that requires it to submit data for tracking Passport students. The Passport Tracking System collects information on (1) the number of Passports awarded by each institution in fall and spring terms of the academic year; (2) the academic progress of transfer students for two terms after transfer in the specified timeframe; and (3) the academic progress of the institution's native students for two terms after earning a Passport to provide a point of baseline comparison with those students receiving a Passport. Participating institutions received an *Academic Progress Tracking Handbook* with full details of the Phase I reporting process.

In Phase I of the initiative, each Passport institution is using a customized version of the Passport Data Collection Tool (Excel template) to enter aggregate data on the institution's students. No personally identifiable information is collected in this process. Completed data files are returned to the Passport Central Data Repository. Initial reporting, with details on a single semester of academic progress, was completed in November 2014. A summary report and analysis of this data was presented to the Passport Review Board (PRB) in February 2015 and customized institution-specific reports were provided to each Passport signatory institution in March 2015. The Passport Tracking System was set up for the CDR to receive data from Phase I participating institutions each November and provide reports to the PRB and individual institutions annually.

The Data Collection Tool used for inaugural (AY2013-2014) reporting was an Excel file containing four tabs: (1) Instructions; (2) Passports Awarded; (3) Transfer-Academic Progress; and (4) Native-Academic Progress.

Tab 1: Instructions. Provides specific instructions and contact information.

Tab 2: Passports Awarded. Reports the number of Passports the institution has awarded in the fall and spring terms of a specific academic year, and the mean number of credits earned when the Passport was awarded.

Tab 3: Transfer - Academic Progress. Reports data on students who transferred to the institution from any other Passport institution during a specific academic year – regardless of whether they earned a Passport – as well as students who transferred from non-Passport institutions. The data elements in this tab include the number of students who transferred to the institution; if they transferred with or without a Passport; the total (aggregate) number of credits attempted with grades A, B, C, D, F, and P; the number of credits started but not earned, DNF; the weighted average GPA for the credits earned; and the average number of credits earned. The last row – TRANS – is for all students who transferred from non-Passport institutions, which provides a baseline for comparison.

Tab 4: Native - Academic Progress. Reports data on the academic progress of native students (first-time enrolled, non-transfer students) – both those who earned a Passport at the institution and those who did not earn a Passport. Reporting covers the academic progress of these students for a specific timeframe: two terms after the student was awarded the Passport. The data elements in Tab 4 are similar to those requested in Tab 3: the number of native students who earned or did not earn a Passport; the number of credits attempted with grades A, B, C, D, F, and P, and the number of credits started but not earned, DNF; the weighted average GPA for the credits earned; and the average number of credits earned.

Data Processing and Reporting Details: Pilot
The reporting process for the 16 institutions participating in the pilot phase of the project was completed in the fourth quarter of 2014. The completed Excel templates for each institution were loaded into a secure SQL database in the CDR at Utah State University. Initial reports and custom data visualizations were generated in January 2015; reviewed by WICHE staff, stakeholders, and the PRB; and final reports were sent to the PRB in February 2015, with reports to individual institutions sent in March 2015.

Data Processing and Reporting Details: Phase I
The Data Collection Tool being used for AY 2014-2015 reporting has been expanded to seven tabs, to accommodate the need for two terms of reporting for each cohort of transfer students (the first reporting included only a single semester of data): (1) Instructions; (2) Passports Awarded; (3) Spring 2014 Cohort, 2nd term; (4) Fall 2014 Cohort, 1st term; (5) Fall 2014 Cohort, 2nd term; (6) Spring 2015 Cohort, 1st term; (7) 2014-2015 Native Academic Progress. The three additional Tabs added to the template (#4, #5, and #6) follow the structure outlined in Tab 3, above. Additional details, including the identification of specific cohorts and semesters of reporting, are required to effectively track academic progress in Phase I.

PRIVACY AND SENSITIVE DATA ISSUES & RIGHTS MANAGEMENT

All data collected in Phase I is aggregate data. The aggregate information is stored on the secure computer system at the CDR. Access to data is limited to only those authorized personnel at the CDR who need the data to perform their official duties. Institution-specific reports are generated from this data, however, data is never transferred between institutions, and data is never stored on portable media (e.g., external hard drives, USB storage devices, or portable computers). The data is backed up as part of an overall resumption of business plan. The submitted summary information is maintained at the request of WICHE. Reports are generated showing the various relationships of the data.

Institutions may access their institution-specific aggregate data at any time by making a request to the CDR. Institutions are not permitted to access the data of other participating Passport institutions.

With the completion of the Passport framework of nine knowledge and skill areas, the Passport Phase I will be phased out. Starting in fall 2016 Passport institutions will award the LDGE Passport to students who achieve the learning outcomes in all nine areas. The CDR will maintain data collected for Phase I for 10 years after the move to Phase II of the Passport.

PHASE II

INTERSTATE PASSPORT DATA DESCRIPTION

Phase II of the Data Management Plan addresses the needs of the project as it expands and grows to scale. As participation expands beyond the 16 initial signatory institutions, WICHE, key stakeholders and the CDR have recognized the difficulties in scaling data collection, security, and management using an Excel template-based system. Phase I data management is a design that worked well for the pilot: easily customizable and providing low-risk data collection (aggregate data only) and a low barrier of entry for initial signatories. Although the reporting tool and SQL data structure at USU has the potential to handle more institutions than are currently enrolled in the pilot, all current stakeholders have agreed that a more permanent and scalable solution is needed. The custom database in the CDR has been set up to collect and store aggregate panel (multi-year) data for all Passport reporting institutions. In this way, multi-year and multi-institutional analysis can be generated for review by the PRB, key stakeholders, and funders. With the addition of a national data partner who can handle data collection and institutional reporting at scale, the CDR is still well positioned to receive aggregate data reporting from that partner to use for overall program and outcome analysis.

The design of the Passport includes three important services involving student data: the ability for (1) receiving institutions to verify that a transfer student has earned a Passport at his/her sending institution and when; (2) sending institutions to learn about the academic success of their former students to use in continuous improvement efforts; and (3) the Passport Review Board to make informed decisions about Passport operations and policies based on this aggregated information.

The best solution for secure, nationally scalable data management is to leverage an existing system already used and trusted by higher education institutions, both public and private, throughout the U.S. In reviewing the national landscape, there are only a few alternatives. The Federal IPEDS system is used by practically all higher education institutions in the U.S. However, IPEDS is poorly suited as a "data partner" for this type of initiative. The second most ubiquitous national data partner is the National Student Clearinghouse (NSC). The NSC was founded as a non-profit organization by the higher education community in 1993. Currently, the NSC counts as participants more than 3,600 colleges and universities, enrolling 98 percent of all students in public and private institutions in the U.S. The NSC performs more than 700 million electronic student record verifications annually.

The NSC is also perhaps best suited as a data partner for the Passport because of its focus on credential reporting and verification (e.g., *Degree Verify)*, data exchange (e.g., *Electronic Transcript Exchange Registry, Reverse Transfer,* and *Transcript Services)*, and research services. By leveraging existing file structures and standards, systems for data submission and verification, and NSC's system management and controls, WICHE can simultaneously provide secure national data collection and access, ease reporting for Passport institutions, and enable more detailed data collection and reporting. The file formats (extracts) and data submission methods for NSC are familiar to NSC partner institutions (which is to say, almost all higher education institutions in the U.S.). By piggy-backing on those systems and file formats, the Passport Institutions will be able to report detailed, student-level data and gain easy verification of the Passport status of individual students who transfer between institutions.

In the Phase II of Data Management, institutions will report on students who receive a Passport through a slightly modified version of NSC's existing service *Degree Verify* that is being labeled ***Passport Verify***. With

funding from the Gates Foundation, WICHE entered into an agreement with NSC to conduct a pilot project with a manual prototype of Passport Verify—verifying that a student has earned a Passport. With new funding from the U. S. Department of Education's First in the World grant, WICHE will contract with NSC to build an automated version of Passport-Verify. Participating institutions will be able to access this service 24x7 at no cost to verify the Passport status of any transfers enrolling.

With regard to Academic Progress Tracking, the current proposal calls for institutions to submit de-identified data to the NSC using a slightly modified version of its *Reverse Transcript* file format and submission process. All student-level data remains the property of the submitting institution. The NSC, in turn, will use the information from all Passport participants to generate institution-specific annual reports with aggregate data on the academic progress of students who transfer from the sending institution to another Passport participant institution. In addition, the NSC will generate annual reports of aggregate data that will be sent to the CDR for analysis and reporting to the PRB, which will audit and evaluate the overall results of the initiative.

DATA ACQUISITION, INTEGRITY AND QUALITY

Data Exchange and Usage. For Passport Verify, registrars at Passport institutions have been briefed on the process, in which they will upload data on Passport students to NSC in the same fashion that they currently upload StudentTracker data to NSC, via a special secure FTP account (the first upload will take place in December 2015). Data elements mirror the elements included in NSC's traditional credential verification service, *Degree Verify*, and will include the student's name, institution awarding the credential [Passport], and the term the Passport was awarded. This student-identifiable information, like in NSC's *Degree Verify*, is considered directory information (DIRINFO) under FERPA requirements, is covered under directory information disclosure, and does not require direct student consent. It remains the responsibility of an institution to tell NSC that a student has opted out of directory information, just like with *Degree Verify*.

For Academic Progress Tracking, receiving institutions will submit to the NSC de-identified academic record data on Passport transfer students and non-Passport transfer students for each of the first two terms after transfer to the institution, and also data on native students for two terms after the Passport is earned. Institutions retain ownership of the information submitted to NSC, and can request that information at any time. NSC will provide only aggregate data in its annual reports to Passport signatory institutions, specifically sending institutions. Receiving institutions, by signing the Passport Network Memorandum of Agreement (MOA), agree to share student academic progress data on Passport students and aggregated academic progress data of transfer students. Access to any data generated by any part of the Passport Network will be granted only to institutions, systems or entities that have signed a Passport Network MOA, are employed by the Passport Network, or are members of the Passport Review Board.

Consent for Data Exchange and Usage. By virtue of accepting an award as a Passport student, the student consents to the use of individual academic data only to the extent that is described in the Passport agreements. This data will be accessed and used only by Passport institutions and the Passport Review Board, without student identifiers attached to individual student data. Any Passport institution shall inform NSC if a block is to be placed on any student's academic data. In no case will any student's past, current or future address, phone numbers of any kind, or any other contact information be released to any Passport Network entity or any entity outside the Passport Network unless both the institution and the student have opted into such a service.

Data Submission: Academic Progress Tracking. At the end of each academic term, Passport Institutions will send NSC the de-identified data outlined in Appendix C: *Passport Data Elements for Passport Verify and Academic Progress Tracking*. They will upload this de-identified student-level data to NSC in the same fashion that they currently upload StudentTracker data to NSC, via a special secure FTP account. Because of the additional detail provided in this reporting, additional aggregate analysis—not currently available to pilot institutions—will be provided. The additional dimensions reported as a part of the de-identified student-level data include Pell recipient (low-income), gender and race/ethnicity. Definitions for these elements follow the commonly accepted IPEDS definitions. Data will be provided for each student in four cohorts (outlined on page 5 above). At the end of each term, each Passport Institution will send to NSC the data outlined in Appendix B. NSC will enter the academic progress data into the Passport database. As stated above, uploads will consist only of de-identified data unless an institution and its students amend their agreement and opt into the use of identifiable data for institution-specific custom reports/services to be offered in the future. Such a change requires the affirmative "opt-in" of each student whose information would be subject to disclosure, and a formal revision to the institutional MOU with WICHE to ensure compliance with all relevant privacy laws.

Data Request Queries. Once each academic year, NSC will compile and sort the data received from the Passport institutions and generate customized institution-level reports with aggregated data on students from each Passport sending institution. NSC will deliver to each Passport sending institution its own custom report, and will send copies of these reports to the PRB. Individual queries for Passport data will not be necessary because each Passport sending institution will automatically receive a report on the aggregated academic progress of its former Passport students. Also once each academic year, NSC will provide a report to the CDR that aggregates the results of the individual institutions currently participating in the Passport . Finally, in Phase II, as submitting institutions retain ownership of the data submitted to the NSC, they will always be able to access and query that data for their own internal analysis and program improvement. Eventually custom reports and custom report packages will be offered to sending institutions.

Privacy and Data Security. Details of NSC's comprehensive, industry-leading security program can be found in Appendix A: *National Student Clearinghouse Security Program Overview*. NSC is a recipient of iKeepSafe's FERPA Badge, signer of the ***Student Privacy Pledge***, and an official supporter of the ***Student Data Principles***.

CENTRAL DATA REPOSITORY REPORTS

In Phase I Data Management, the Central Data Repository collects and organizes the data supplied by the participating institutions and prepares customized reports for each, as well as a composite report for the Passport Review Board. In Phase II Data Management, the CDR will focus on evaluation of the aggregate results from the initiative while all institution-level reporting shifts to the National Student Clearinghouse.

CDR/NSC Reports to Passport Sending Institutions. After receiving data from all Passport institutions, the data partner prepares reports for the sending institutions – those that had students transfer to other Passport institutions. These reports provide aggregate (de-identified) details on student performance after transfer, including aggregate data on students who transferred from non-Passport institutions, to provide a comparative baseline. Sending institutions receive reports on grades by percentage, weighted average GPA, and number of credits attempted per term from every Passport institution to which their students transferred. These reports inform sending institutions of how their students fared after they transferred. Over time this will become a richer illustration. The data reports will be delivered to Passport institutions in January or February each year.

CDR Reports to Passport Review Board. The CDR aggregates and compiles all data submitted by Passport institutions to create summary reports on all Passport students: the total number of Passports awarded, grades by percentage, weighted average GPA, and total average number of credits attempted per term. These reports will be delivered to the Passport Review Board in the first quarter of each year in the form of the Passport Annual Report.

Members of the Passport Review Board include the Passport State Facilitator from each participating state as well as other at-large members with specific expertise. The PRB is responsible for reviewing data provided through the Central Data Repository to assess the Passport's effectiveness. The data provided by each Passport institution is vital to the PRB's efforts to monitor the quality of the project and to make adjustments in the process. These reports will not only reveal the level of participation by students and institutions and how students perform after transfer, but also will inform the Board's work on the Passport process and areas that may need strengthening.

LEGAL FRAMEWORK FOR THE PASSPORT

Each Passport institution signs a Memorandum of Agreement, for a five-year term, which outlines the conditions and responsibilities of the institution in the implementation of the Passport. The MOA is signed by the institution president, provost, commissioner or similar individual with proper authority. Specific to the awarding of Passports and data tracking, the MOA states that the institution:

- Agrees to track subsequent progress of students who enter with a Passport and exchange appropriate transfer data with relevant partner institutions; use the data collected and exchanged in a self-examination and continuous improvement process, and commit to documenting and sharing student progress and transfer data.

In addition, the Passport Facilitator in each state, as part of his/her contractual scope of work, is required to:

- Work with registrars at partner institutions to implement the notation process for Passport achievement on student academic records.
- Work with institutional researchers and/or others responsible for implementing data collection on Passport student academic progress and developing communication processes for continuous improvements.
- Ensure that participating institutions supply aggregate data for analysis on the established timeline.
- Monitor reports from the Central Data Repository on the performance of Passport students based on data collected from participating institutions through the tracking process.

See a sample Memorandum of Agreement at http://www.wiche.edu/info/passport/agreement.

Appendices

Appendix A

NSC Security Program Overview V1.1

NATIONAL STUDENT CLEARINGHOUSE®

National Student Clearinghouse Security Program Overview

Version 1.1

August 5, 2014

NATIONAL STUDENT CLEARINGHOUSE

2300 Dulles Station Blvd., Suite 300, Herndon, VA 20171

Version Control

Date	Author	Version
11/26/2012	Information Security Team	1.0
08/05/2014	Information Security Team	1.1

Introduction

Since our inception in 1993, the National Student Clearinghouse (NSC) has been extremely proactive in the actions it has taken to ensure the security and confidentiality of the information in our care. During our almost 20-year history, we have maintained the confidentiality and privacy of the now more than 100 million student records entrusted to us without a breach of security.

Our multi-faceted security program is based on a defense in depth approach to prevent unauthorized data access and protection against threats and hazards to the security and integrity of NSC data and facilities. Our security program consists of the following elements:

System Management & Controls

Risk Assessment: NSC management performs periodic risk analysis of operational and technological risks. Risks are identified and ranked, and mitigation steps are developed.

System Life Cycle Management: Formal system change policies and procedures exist addressing the classification of production systems, separation of systems and duties, definition of system changes and change windows, and requirements for documentation, notification and authorization.

System Security Certification: The NSC has been certified by a Qualified Security Assessor (QSA) in the Payment Card Industry Data Security Standards (PCI-DSS), which are the unified base requirements for all credit card association data security programs. Association data security programs, such as Visa CISP, MasterCard SDP, American Express and Discover Card, all require PCI-DSS. The NSC uses a certified vendor, TrustWave, for its PCI-DSS compliance program. TrustWave Site Certification fulfills all requirements of PCI-DSS, Visa CISP, MasterCard SDP, American Express DSS, and Discover Card programs.

System Security Accreditation & Assurance: In addition to its ongoing PCI DSS certification process, the NSC contracts annually with third-party security firms to perform an exhaustive security assessment, including external and internal network penetration testing. NSC staff members responsible for managing systems subscribe to Department of Homeland Security (DHS) United States Computer Emergency Response Team (U.S. CERT) advisories, System Administration, Networking and Security (SANS) Institute advisories, and other relevant sources providing current information about security vulnerabilities. In addition, the NSC also employs staff with current information security certifications, such as the Certified Information Systems Security Professional (CISSP) to ensure that it stays current with industry best practices.

System Security Plans: A formal information security plan, which covers all aspects of information security, is in place at the NSC. It is reviewed by management on a regular basis and updated as needed.

Operational Controls

System Security: Multiple levels of system security policies, procedures and controls are in place to secure NSC systems, including physical, logical, network, and access control.

Data Security: Access to data on NSC systems is protected by multiple layers of policies, procedures and controls. Users are only granted access to data that is necessary to perform the duties of their position. Access is granted by written authorization and controlled by policy.

Clearinghouse Security Program

User Administration: Policies and procedures are in place for administering user access, including both internal and external users.

Separation of Duties: Procedures regarding critical duties have been established to ensure proper checks and balances are in place. Through our annual audit, conducted by an independent third party, operational procedures and internal controls are reviewed to ensure adequate separation of duties. One of the primary purposes of our annual audit is to identify lapses in processes and risk vulnerabilities. This audit is conducted in accordance with U.S. Department of Education (ED) guidelines and is supplied to ED. Any recommended organizational or procedural changes appear in the auditor's report and are reported to our board of directors. Additionally, the NSC asks each of its guarantor agency clients (which includes every guarantor agency in the country) to identify potential risk situations at least twice a year. We are also periodically audited by ED and subject to individual audits by the more than 3,300 schools to which we provide services.

Personnel Security: All employees are issued photo identification badges for monitoring and providing access to NSC premises. Non-employees, such as consultants, working at the NSC are issued a temporary security badge. Photo identification or security badges are required for access to all office space occupied by the NSC. The NSC's Computer Room is located within our locked suite; access to this area is limited to authorized staff as is access to storage areas containing confidential information. Visitors are escorted by staff while on the NSC's premises. Access to the building during non-business hours requires an authorized photo identification badge. All building entrances and exits are monitored with video surveillance equipment and require a key card. Unauthorized access to any NSC suite triggers an alarm. A security company monitors the doors and has been provided with telephone notification procedures.

Security Awareness, Training & Education: Training in information security is provided to all employees upon hire; additional information is provided on a regular basis. The NSC's written operating policies and procedures include technical, physical and operational safeguards. All staff (i.e., employee, contractor, consultant, temporary, volunteer, intern, etc.) must comply with the NSC information security policies; those who do not are subject to disciplinary action up to and including termination. Operational safeguards governing the handling of sensitive information are initiated through risk assessment by the NSC's Information Security Committee, comprised of representatives from all the NSC's operational units.

Security Incident Handling: The NSC has procedures in place to instruct employees how to properly address security concerns. Depending on the situation, these procedures include notifying a supervisor, our internal Computer Security Incident Response Team (CSIRT), and Human Resources, as appropriate. In addition, a written information security incident response plan is in place.

Physical & Environmental Security: Procedures are in place to instruct employees how to react and handle any threat of which they become aware. If management becomes aware of a threat, procedures are in place to notify the staff in a timely manner.

Configuration Management: Formal system change policies and procedures are in place to address system configuration management, including authorization and separation of duty. Procedures also exist that specify the standard configuration of NSC systems.

Media Protection: Policies and procedures are in place to address media handling, labeling, release and destruction.

Technical Controls

Identification & Authentication Methods: User identification and authentication controls are in place for all NSC systems. Specific security policies address user access, password management, and authentication.

Logical Access Controls: Logical access controls are in place for all NSC systems. All systems require a unique user login. Access is granted by written authorization and only for access to necessary systems and data.

System & Communication Protection: All systems are protected by industry recommended practices, such as firewalls, access lists, virtual LANs, intrusion detection and prevention, DMZ's, system patches, anti-virus software, proxy servers, DLP, etc.

Change Control: Formal system change policies and procedures are in place addressing the classification of production systems, separation of systems and duties, definition of system changes and change windows, and requirements for documentation, notification and authorization.

Cryptographic Technologies: Cryptographic technologies are utilized to protect data in NSC systems including web servers, file transfer servers, database servers, backup software, etc. The NSC supports several encryption options for secure file transfer. Production system backup tapes that are transported off-site are encrypted.

Audit Trails: Our application systems maintain audit trails for various events that occur in the system, including history of data exchanges, history of each individual record as it is reported to various entities, and history of specific data elements as they are changed in the database. In addition, system-level audit trails are monitored and reviewed, including user authentication, network access, firewall traffic, etc.

Information Security

The NSC does not sell, lease, provide or otherwise share individual information with any unauthorized third parties. We utilize numerous measures to protect our information, including:

- Internal Systems
    - All servers are located in a dedicated, locked computer room with restricted access.
    - All computers and internal network access points are password protected with stringent password creation and expiration rules.
    - Internal computers are isolated from external networks via a firewall.
    - School and member data is loaded into a relational database.
        - Database security is deployed to restrict access.
        - The physical machine is password protected.
        - Backup tapes are encrypted, labeled "Confidential," and stored in a secure off-site facility.
    - Internal applications that access the database are password protected.
- Secure File Transfer (FTP over SSL/SSH)

  - User accounts are initially established by Customer Service. User IDs and passwords are communicated over the phone.
  - The Secure FTP server is located in the "DMZ" network segment.
  - The physical machine is dedicated to Secure FTP services and has been hardened to allow only those services to run.
  - Session transmission is encrypted using 256-bit Secure-Socket Layer (SSL) connections.
  - The NSC utilizes additional encryption software that encrypts files at rest and in transit using 256-bit Advanced Encryption Standard (AES).
  - The encryption standards utilized are compliant with the U.S. Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*.
  - The Secure FTP server performs virus scanning on all file transfers.
- Web Access
  - Web access accounts are established by Customer Service. User IDs and passwords are communicated over the phone.
  - Log-in and application session pages are all encrypted via 256-bit SSL.
  - Transaction details are logged to a database.
  - Web servers are located in the "DMZ" network segment.
  - Web servers are protected with current anti-virus definitions.
  - Web servers are scanned regularly to ensure no known vulnerabilities exist.

Disaster Recovery & Backup

The NSC has a formal business continuity plan in place that addresses employee workspace (i.e., office space, furniture, printers, workstations, etc.) and system recovery procedures, including backup/restore procedures. In the event of a disaster, employees would be directed to our contracted alternate facilities, and our production systems will be restored at a contracted recovery hot site.

Our disaster recovery site is provided by a reputable contracted service provider. We conduct annual tests of our disaster recovery procedures. The business continuity plan and disaster recovery procedures are updated as needed.

Appendix B

Passport Signatory Institutions, CDR Data Elements (Phase I), and

Acronyms and Definitions

Current Passport Signatory Institution Code Table	
Institution Codes	**Institution Title**
HILCC	Hawaii – Leeward Community College
HIUHWO	Hawaii – University of Hawaii, West Oahu
NDLRSC	North Dakota – Lake Region State College
NDNDSC	North Dakota – North Dakota State University
NDNDCS	North Dakota – North Dakota College of Science
NDVCSU	North Dakota – Valley City State University
ORBMCC	Oregon – Blue Mountain Community College
ORWOU	Oregon – Western Oregon University
UTDSU	Utah – Dixie State University
UTSLCC	Utah – Salt Lake Community College
UTSC	Utah – Snow College
UTSUU	Utah – Southern Utah University
UTUVU	Utah – Utah Valley University
UTUU	Utah – University of Utah
UTUSU	Utah – Utah State University
UTWSU	Utah – Weber State University
WYLCCC	Wyoming – Laramie County Community College
TRANS	Transfer Students Without a Passport that are not reported separately

Passport Extract Fields Reported by Signatory Institutions			
Order	**Field**	**Data Type**	**Additional Information**
1	Your Institution Code	Character (10)	e.g., "UTUSU"
2	Your Institution Name	Character (80)	e.g., "Utah State University"
3	State of Sending Institution	Character (2)	e.g., "UT"
4	Sending Institution (Code)	Character (10)	e.g., "UTSLCC"
5	Transferred with the Passport?	Character (1)	e.g., "Y" or "N"
6	Number of Students Transferred	Number (Integer)	e.g., "399"
7	Number of credits of A	Number (Integer)	e.g., "3311"
8	Number of credits of B	Number (Integer)	e.g., "2307"
9	Number of credits of C	Number (Integer)	e.g., "1099"
10	Number of credits of D	Number (Integer)	e.g., "354"
11	Number of credits of F	Number (Integer)	e.g., "484"
12	Number of credits of W	Number (Integer)	e.g., "177"
13	Weighted Average GPA	Number (Float)	e.g., "2.81"
14	Average Number of Credits	Number (Float)	e.g., "10.78"

Acronyms and Definitions	
Central Data Repository (CDR)	The Passport's CDR provides additional analysis to WICHE on the aggregate data developed by NSC for the participating institutions and for the PRB.
Degree-Seeking Student	A student who has declared he/she is seeking a degree (associates or bachelors).
De-Identified Student Records	Individual student records with all identifying student information removed such as student name, ID, SSN, etc. All records submitted by Passport institutions for the Passport Academic Progress Tracking are de-identified.
Native Student	Students awarded Passport by the reporting institution which is also a receiving institution for Passport and non Passport transfer students.
Passport Institution	Institutions approved for participating in the Passport program. These institutions are both sending and receiving institutions. NSC receives data from PRIs annually. NSC aggregates and sorts this data and then sends a customized report to the relevant PSIs annually.
Passport Receiving Institution (PRI)	The institution to which a student transfers. This is the reporting institution which also awards Passports to its native students who do not transfer.
Passport Review Board (PRB)	The policy making body of the Passport program which approves all institutions for Passport status and monitors the performance of these institutions. NSC prepares aggregate reports for the PRB annually.
Passport Sending Institution (PSI)	The institution from which a student transferred. Transfer students may include those with and without a Passport.
Passport Student	A student who has earned a Passport by completing the institution's Passport Block. This student may remain at the institution where he/she earned the Passport or transfer to another institution.
Transfer Student	A student who transfers to a receiving institution with or without a Passport.
Weighted GPA for one term after transfer	The student's average GPA based on grades and the number of credits earned during the first term after transfer. Students are separated by those with a Passport and those without a Passport.
Weighted GPA for two terms after transfer	The student's average GPA based on grades and the number of credits earned during the second term after transfer. Students are separated by those with/without a Passport.
Weighted GPA for first term after earning Passport	The student's average GPA based on grades and the number of credits acquired during the first term after earning the Passport.
Weighted GPA for second term after earning Passport	The student's average GPA based on grades and the number of credits acquired during the second term after earning the Passport.
Western Interstate Commission for Higher Education (WICHE)	WICHE, a regional compact established by the U.S. Congress in the 1950s to share information and resources among institutions within its region, manages the nationwide Passport program.

Appendix C

Passport Data Elements for Passport Verify and Academic Progress Tracking

Passport Verify Data Elements for Submission to NSC

Following are the data elements and specifications for Passport Verify, a new service to be offered to Passport institutions by the National Student Clearinghouse. The Clearinghouse launched a pilot project for Passport Verify in fall 2015 in order to test the data submission process and to confirm the data elements and specifications for analysis and reporting. The file format is based on NSC's Degree-Verify that most institutions already use. Passport institutions upload data via secure FTP accounts at the end of each term on the students awarded a Passport. The data elements below may be slightly modified at the conclusion of the pilot phase.

STEP 1: In row 1, enter HEADER record for Columns A-I

For the Passport, provide data for highlighted elements only.

Column	Max. Character Count	Description	Required?
A	3	**Record Type. Enter "G1" without quotation marks.**	Required
B	6	**Your 6-digit school code (e.g. 001234).**	Required
C	2	**Your 2-digit branch code (e.g. 00).**	Required
D	80	**Your school name.**	Required
E	15	Filler.	n/a
F	1	**Standard report flag. Enter "D" without quotation marks.**	Required
G	8	**Date of transmission (YYYYMMDD format).**	Required
H	80	**Time period for which passports are being awarded (e.g. Fall 2015).**	Required
I	3645	Filler.	n/a

STEP 2: Starting with row 2, enter student DETAIL records for Columns A-BD

Each student's individual information should be entered in its own row.

Column	Max. Character Count	Description	Required?
A	3	**Record Type. Enter "DD1" without quotation marks.**	Required
B	9	**Social Security Number without dashes.**	Required
C	40	**First Name.**	Required
D	40	Middle Name (If full name not available, use middle initial).	Optional
E	40	**Last Name.**	Required
F	5	Name Suffix.	Optional
G	40	Previous Last Name.	Optional
H	40	Previous First Name.	Optional
I	8	**Date of Birth (YYYYMMDD format).**	Required
J	20	College Student ID.	Optional
K	1	**Level Indicator. Enter "G" without quotation marks.**	Required
L	80	**Passport Title. Enter "Passport" without quotation marks.**	Required
M	50	School/College/Division Awarding Passport.	Optional
N	60	Joint School/College/Division Awarding Passport.	Optional
O	8	**Date Passport Awarded (YYYYMMDD format).**	Required
P	80	**Major Course of Study 1. Enter "GE" without quotation marks.**	Required

Column	Max. Character Count	Description	Required?
Q	80	Major Course of Study 2.	Optional
R	80	Major Course of Study 3.	Optional
S	80	Major Course of Study 4.	Optional
T	160	Filler.	n/a
U	80	Minor Course of Study 1.	Optional
V	80	Minor Course of Study 2.	Optional
W	80	Minor Course of Study 3.	Optional
X	80	Minor Course of Study 4.	Optional
Y	160	Filler.	n/a
Z	80	Major Option 1.	Optional
AA	80	Major Option 2.	Optional
AB	160	Filler.	n/a
AC	80	Major Concentration 1.	Optional
AD	80	Major Concentration 2.	Optional
AE	80	Major Concentration 3.	Optional
AF	280	Filler.	n/a
AG	6	NCES CIP Code for Major 1.	Optional
AH	6	NCES CIP Code for Major 2.	Optional
AI	6	NCES CIP Code for Major 3.	Optional
AJ	6	NCES CIP Code for Major 4.	Optional
AK	20	Filler.	n/a
AL	6	NCES CIP Code for Minor 1.	Optional
AM	6	NCES CIP Code for Minor 2.	Optional
AN	6	NCES CIP Code for Minor 3.	Optional
AO	6	NCES CIP Code for Minor 4.	Optional
AP	120	Filler.	n/a
AQ	50	Academic Honors.	Optional
AR	196	Filler.	n/a
AS	50	Honors Program.	Optional
AT	100	Filler.	n/a
AU	150	Other Honors.	Optional
AV	8	Attendance From Date (YYYYMMDD format).	Optional
AW	8	Attendance To Date (YYYYMMDD format).	Optional
AX	1	**FERPA Block. Enter “Y” or “N” without quotation marks.**	Required
AY	1	School Financial Block. Enter “Y” or “N” without quotation marks.	Optional
AZ	100	Filler.	n/a
BA	50	Name of Institution Granting Degree, if it is different than the school name in the header.	Optional
BB	1	Reverse Transfer Flag. Enter “Y” or “N” without quotation marks.	Optional
BC	1	Certificate Type.	Optional
BD	553	Filler.	n/a

STEP 3: After the last student row, enter Trailer record for Columns A-C

Column	Max. Character Count	Description	Required?
A	3	**Record Type. Enter "DT1" without quotation marks.**	Required
B	10	**Total Record Count. Equals the number of student detail records plus two (header and trailer records are included in total).**	Required
C	3827	Filler.	n/a

Academic Progress Tracking Data Elements for Submission to NSC

Following are the data elements and specifications under consideration for the Passport Academic Progress Tracking, a new service to be offered to Passport institutions by the National Student Clearinghouse that is based on the NSC Reverse Transfer model. Passport institutions will upload data via secure FTP accounts at the end of each term on the students awarded a Passport and on the academic progress of relevant transfer and native students. The shaded elements on the next page are not required for the Passport, but may be submitted by the institution if both the institution and its student opt to provide this information. Institutions participating in NSC's Reverse Transfer may want to take advantage of this option.

File Format: Tab Delimited File				
Academic Tracking System				
Field Description	**Length**	**Data Type**	**Required**	**Notes**
Header				
Record Type Enter "PSAP1" without quotation marks	5	AN	Yes	
Your 6-digit school code (e.g., 001234).	6	N	Yes	
Your 2-digit branch code (e.g., 00).	2	N	Yes	
File Certified Date	8	N	Yes	
Client File ID	50	N	Yes	
Detail				
Record Type "PD1"	3	AN	Yes	
Passport Reporting Institution Auto-Generated Unique Student ID	80	AN	Yes	
Year of Birth (YOB)	8	N	Yes	
Low income	3	A	Yes	Yes, No or null? Provide list of valid values
Gender	20	AN	Yes	Provide list of valid values
Race/Ethnicity	20	AN	Yes	Provide list of valid values
Military/Veteran	3	A	Yes	Yes, No or null? Provide list of valid values
First Generation	8	Char	Yes	Yes, No or null?
Date Admitted to Reporting Institution	8	N	Yes	
Transfer Student	3	A	YES	Yes, No or null? Provide list of valid values
Sending Institution OPEID remain (Original School?)	6	N	Yes, if transfer student	The name can be changed to Previously attended or Previous institute OPEID
Sending Institution OPEID Branch Code	2	N	Yes, if transfer student	The name can be changed to Previously attended or Previous institute branch code
Total GPA earned at Sending Institution	4	N	Yes, if transfer student	The name can be changed to GPA at Previously attended or Previous institute
Total Credits earned at Sending institution	10	N	Yes, if transfer student	The name can be changed total credits at previously attended or Previous institute
Passport	3	A	Yes	Yes, No or null? Provide list of valid values

Field Description	Length	Data Type	Required	Notes
Date Passport Awarded	8	N	Yes if Passport Flag is Y or Yes	
Degree Granted by Institution Named in Header	3	A	Yes	Yes, No or null? Provide list of valid values
Date Degree Awarded YYYYMMDD	8	N	Yes if Degree flag is Y or yes	
Type of Degree	20	Char	Yes if Degree flag is Y or yes	Provide list of valid values
Major Course of Study	20	Char	Yes	Provide list of valid values
Course Name	20	Char	Yes	
Course Number	20	Char	Yes	
Course-Term Session	20	Char	Yes	
Course Begin Date	8	N	Yes	
Grade Effective Date	8	N	Yes	
Number of Credits	20	N	Yes	
Credit Description	20	N	Yes	
Host Student ID	20	Char	Yes	This Identifiable student-level information in the shaded area is not required to participate in the Passport unless both an institution and its students opt to share this information. Institutions participating in NSC's Reverse Transfer may wish to do so.
SSN	9	N	No	
ITIN	9	N	No	
First Name	60	AN	No	
Middle Name	60	A	No	
Last Name	60	A	No	
Suffix	10	AN	No	
Street line 1	30	Char	No	
Street line 2	30	Char	No	
City	20	Char	No	
State	2	A	No	
Zip	10	Char	No	
Country	15	A	No	
Student Phone Number	20	Char	No	
Student Email	255	Char	No	
Trailer Record Layout				
Record Type Enter "PST1" without quotation marks	4	N	Yes	
Total Record Count	No Limit	N	Yes	