InCommon Participant Operational Practices (POP)

1. Federation Participant Information

1.1 The InCommon Participant Operational Practices information below is for:

InCommon Participant organization name: NFORMD.NET dba Student Success

The information below is accurate as of this date: October 22, 2014

1.2 Identity Management and/or Privacy information

Additional information about the Participant's identity management practices and/or privacy policy regarding personal information can be found on-line at the following location(s).

URL(s): http://public.studentsuccess.org/privacy

1.3 Contact information

The following person or office can answer questions about the Participant's identity management system or resource access management policy or practice.

Name: Gene Ginzburg

Title or role: Director of Technology Innovation

Email address: gene.ginzburg@studentsuccess.org

Phone: 412-345-8161 FAX: 412-345-8161

2. Identity Provider Information

Student Success is not an Identity Provider.

3. Service Provider Information

Service Providers are trusted to ask for only the information necessary to make an appropriate access control decision, and to not misuse information provided to them by Identity Providers. Service Providers must describe the basis on which access to resources is managed and their practices with respect to attribute information they receive from other Participants.

3.1 What attribute information about an individual do you require in order to manage access to resources you make available to other Participants? Describe separately for each resource ProviderID that you have registered.

Student Success only requires a unique user identifier in order to provide access to our applications. This identifier is used internally to uniquely identify the individual within the applications and also for reporting. The identifier chosen by the organization using the Student Success training should be one that, when reported back to the organization, can be used in whatever controls and processes required by the organization. The specific attribute is determined by our customer based on their requirements for the use of our applications.

3.2 What use do you make of attribute information that you receive in addition to basic access control decisions? For example, do you aggregate session access records or records of specific information accessed based on attribute information, or make attribute information available to partner organizations, etc.?

Any attributes provided are used solely for the delivery of services to the individual, access to any applications, and for reporting back to the organization. No attribute-related data is ever shared with any other entity.

3.3 What human and technical controls are in place on access to and use of attribute information that might refer to only one specific person (i.e., personally identifiable information)? For example, is this information encrypted?

All implementations of the Student Success system consist of two components: a “front-end” (which is the interface-the end user sees in their web browser) and a “back-end” (which is the application logic and data repository). The front-end is a similar to a dumb-terminal, such that although questions are asked and answered via this interface, no data is ever stored on the front- end (i.e. the web browser or the end user’s computer). These front-end components run a custom web application built using web technologies (e.g., HTML, JavaScript and CSS) that has been designed to securely connect to Student Success’s back-end. The connection between the front-end and the back-end is secured with 256-bit TSL encryption (i.e. https), and user authentication is required to establish the connection. A traditional Cicso firewall sits between the back-end server and the wider Internet, with only the minimal ports open (80 and 443). Additionally, a web application firewall (WAF) operates between the back-end server and the wider Internet. This WAF monitors all traffic and automatically blocks any suspicious traffic. The back-end server is running Red Hat Enterprise Linux OS, Apache web server and a MySQL database server, with a secure certificate for encryption. If a connection between a front-end browser and the back-end server has become inactive for a period of time, the connection is terminated and the client must re-authenticate. All sensitive files and data on the backend are stored in an encrypted format. The database is encrypted using AES 256. The system servers reside in a facility that is certified SSAE 16 / ISAE 3402 compliant (including SAS 70 compliance). All files (programming code) and data on the back-end are backed up to tape nightly, and backups are retained for 30 days.

In addition to the security provided by the Client/Sever technical design, we also have a feature designed to prevent a Client from uniquely identifying the personal data from any individual Participant. For each Client (e.g., each school), an administrator is provided with access to an online portal that provides information about that Client’s Participant’s progress. They have access to a Progress Report, which includes Participant-specific information as discussed above. They also have access to a raw data report that includes all of the de-identified data. The de-identified data does not become available to the Client until at least 100 men and 100 women have completed the program. In addition, each time the full raw data report is opened the information is randomized. These protections ensure that a Client is not be able to review the Participant that have completed the program each day and try to match it up with data in the raw data report, thereby identifying the personal data from any individual Participant. Should a Client not meet the 100 men and 100 women minimum, they are not provided access to the raw data until after all Participants have completed the program, and if the number of completions is still too low at that time, either the demographic data is removed from the raw data file all together or with very small populations, the raw data is not provided at all at.

3.4 Describe the human and technical controls that are in place on the management of super-user and other privileged accounts that might have the authority to grant access to personally identifiable information?

Access to data is tightly controlled and only available to a few select individuals. Interaction with data via regular and privileged accounts is logged and is subject to internal review and auditing policies.

3.5 If personally identifiable information is compromised, what actions do you take to notify potentially affected individuals?

If any Student Success employee suspects that a breech of privacy, disclosure of protected information, or any other security incident has occurred, they will immediately report the suspected breach to the Chief Information Security Officer (CISO). If the CISO determines that a breech has occurred, the CISO will immediately notify all schools that were or may have been included in the breach. The CISO will work with the school to determine the desired course of action of the school and will implement that course of action as soon as possible, but no later than the 5th day on which a security

breach is known. The standard course of action is that each individual whose data was or may have been included in the breach will be directly notified. These notices will be delivered as soon as possible, but no later than the 5th day on which a security breach is known.

The notice will be written in plain language and will include, to the extent possible or available, the following:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach;
- A description of the types of data that were involved in the breach;
- Any steps that individuals who were subjects of the breach should take to protect themselves from potential harm that may result from the breach;
- A brief description of what Student Success is doing to investigate the breach, to mitigate the harm to affected individuals, and to protect against further breaches; and
- Contact procedures for affected individuals to ask questions or learn additional information, including a toll-free telephone number, an email address, a website, or postal address.

4. Other Information

4.1 Technical Standards, Versions and Interoperability

Identify the version of Internet2 Shibboleth code release that you are using or, if not using the standard Shibboleth code, what version(s) of the SAML and SOAP and any other relevant standards you have implemented for this purpose.

Shibboleth 1.3

SAML 2.0

CAS

4.2 Other Considerations

Are there any other considerations or information that you wish to make known to other Federation participants with whom you might interoperate? For example, are there concerns about the use of clear text passwords or responsibilities in case of a security breach involving identity information you may have provided?