Report on National Student Clearinghouse's Verification Services and Transcript Services Systems Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy Throughout the Period July 1, 2022 to June 30, 2023

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: National Student Clearinghouse ("NSC")

Scope

We have examined NSC's accompanying assertion titled "Assertion of National Student Clearinghouse Management" (assertion) that the controls within NSC's Verification Services and Transcript Services Systems (system) were effective throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that NSC's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

NSC uses subservice organizations to provide data center colocation services, security-as-a-service, and infrastructure monitoring. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at NSC, to achieve NSC's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of NSC's controls. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

NSC is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that NSC's service commitments and system requirements were achieved. NSC has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, NSC is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve NSC's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve NSC's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within NSC's Verification Services and Transcript Services Systems were effective throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that NSC's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of NSC's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Greenwood Village, Colorado
September 26, 2023

Section 2

Assertion of National Student Clearinghouse Management

National Student Clearinghouse℠

2300 Dulles Station Blvd., Suite 220
Herndon, VA 20171
www.studentclearinghouse.org

Assertion of National Student Clearinghouse ("NSC") Management

We are responsible for designing, implementing, operating and maintaining effective controls within NSC's Verification Services and Transcript Services Systems (system) throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that NSC's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

NSC uses subservice organizations for data center colocation services, security-as-a-service, and infrastructure monitoring. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at NSC, to achieve NSC's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of NSC's controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2022 to June 30, 2023, to provide reasonable assurance that NSC's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of NSC's controls operated effectively throughout that period. NSC's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period July 1, 2022 to June 30, 2023 to provide reasonable assurance that NSC's service commitments and system requirements were achieved based on the applicable trust services criteria.

National Student Clearinghouse

Sincerely,

John Ramsey

John Ramsey
Chief Information Security Officer
National Student Clearinghouse

Attachment A

National Student Clearinghouse's Description of the Boundaries of Its Verification Services and Transcript Services Systems

Type of Services Provided

Founded in 1993 in the Commonwealth of Virginia by the higher education community, the National Student Clearinghouse® (“NSC,” “the Clearinghouse,” or “the Company”) relieves the administrative burdens and costs related to student data reporting and exchange. The Clearinghouse is a 501(c)(4) nonprofit and nongovernmental organization and is the leading provider of educational reporting, data exchange, verification, and research services. NSC’s work — performed in a trusted, secure, and private environment — provides numerous time- and cost-saving benefits to students, schools, administrators, and data requestors (e.g., financial institutions). NSC supports over 3,600 colleges and universities and 22,000 high schools, providing enrollment and degree information to users regularly throughout the year. NSC provides free and low-cost services, saving the education community over $750 million annually. The Clearinghouse’s research arm, the National Student Clearinghouse® Research Center™, a 501(c)(3) nonprofit organization, works with higher education institutions, states, districts, high schools, and educational organizations to better inform practitioners and policymakers about student educational pathways and enable informed decision making.

The Clearinghouse serves as a trusted agent to participating institutions, providing support for their compliance, administrative, student access, accountability, and analytical needs. Services are designed to facilitate compliance with the Family Education Right to Privacy Act (FERPA), the Higher Education Act, and other applicable laws. Clearinghouse services include Data Exchange and Transcript Services (TS), Financial Aid Services, Research Services, Verification Services (VS), and Insights.

Verification Services

VS includes:

- DegreeVerify
- EnrollmentVerify
- DiplomaVerify
- Professional Certification Verifications
- Insights

These services provide users with tools to perform academic verifications of students and alumni and speeds results to requestors.

EnrollmentVerify enables companies that offer products or services that require proof of a student’s enrollment status to query actual college enrollment data online and obtain student status instantly. Users can query up-to-date enrollment data provided exclusively to NSC by its national network of thousands of participating postsecondary institutions.

As the need for financial services grows among underbanked individuals, Insights can be used to regularly monitor enrollment status and determine when students leave college. Users can also find out if, when, and where individuals re-enter college.

Transcript Services

NSC’s Online Transcript Ordering Service allows students and alumni to quickly and securely order transcripts utilizing one of the following delivery methods:

- Mail
- FedEx Corporation/United Parcel Service (UPS)

- Electronic delivery (PDF)

The service is mobile and tablet friendly. NSC's TS also allows for tracking the status of the orders from ordering to delivery. It is a free service to the education industry and relieves schools and universities of the burden of the ordering process. If the schools and universities choose to charge for transcripts, then NSC will manage and fulfill the payment process.

The Components of the System Used to Provide the Services

The boundaries of the VS and TS systems are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the VS and TS systems.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

Verification Services

The VS application is housed on servers located in a third party facility in Ashburn, Virginia, with a DR site in Culpepper, Virginia. The NSC servers are isolated in a locked cage that extends from floor to ceiling in a climate-controlled space.

Services are enabled within the IT environment by a range of applications and hardware.

Transcript Services

The TS application is hosted in a hybrid cloud site. The hosting company is a trusted provider of managed services including cybersecurity and enterprise cloud solutions. The hybrid cloud option enables NSC to leverage its current infrastructure by connecting a co-located dedicated environment to a cloud environment.

Software

Software consists of the programs and software that support the VS and TS systems (operating systems, middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor the VS and TS systems include the following applications:

- Authentication and authorization to the VS and TS systems
- Data storage
- Firewall technology
- Vulnerability scanning tool
- Standard automated application security vulnerability testing
- Vulnerability reporting
- SIEM

- Ticketing system
- IPS
- Backups and storage to secondary data center
- SAN
- IT infrastructure monitoring tool
- Cloud environment monitoring tool

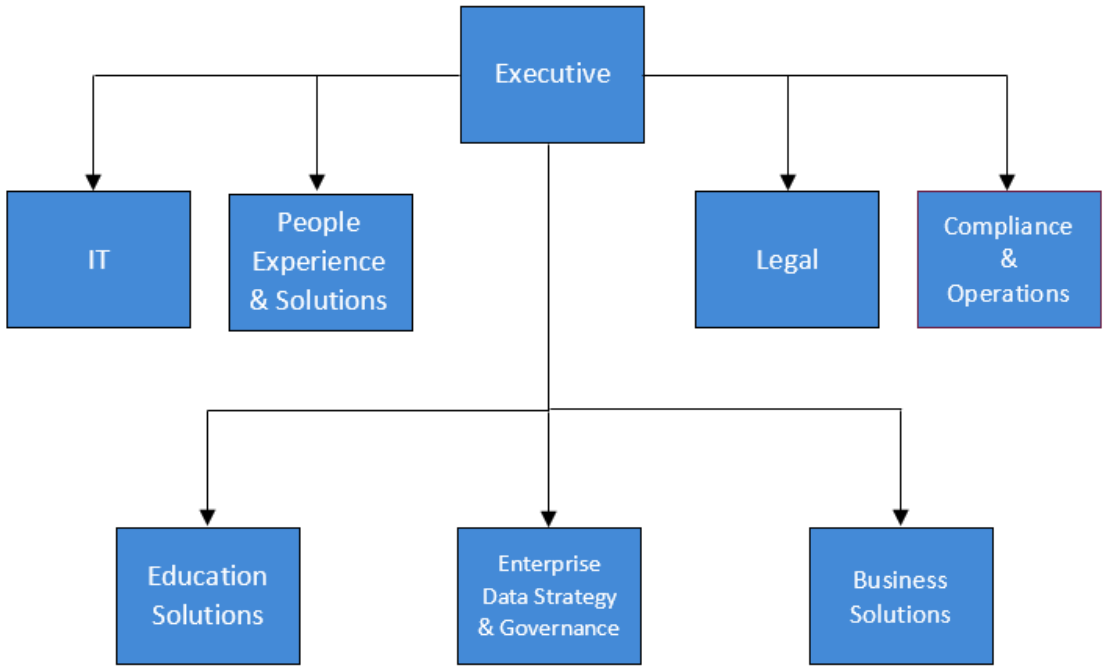
People

The Company develops, manages, and secures the VS and TS systems via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Management	The Office of the President/Chief Executive Officer (CEO) develops, implements, and ensures the timely flow of organizational processes and communications to strengthen and improve coordination between the Executive Management team, member associations, Business Solutions, Education Solutions, board relations, government contacts, the Senior Management team, and staff.
Information Security/Technology (InfoSec/IT)	The IT department consists of the Application Development, Cybersecurity, and other teams. These teams develop and maintain the technology that is essential for running NSC operations (e.g., uploading requests and submissions). They are also responsible for developing, maintaining, and enforcing NSC's Information Security policies. The IT department also performs NSC's monitoring functions. The IT team monitors and reports on known incidents and patches, as well as results from recent vulnerability assessments, and addresses required changes to policies and procedures. Changes are reviewed and communicated during twice-weekly change control meetings or through system alerts.
Compliance and Operations	The Compliance and Operations department provides Tier 1 and 2 support for the services provided to the clients. It helps set up services, trains clients on how to use the products, and provides support throughout the life of the service.
Legal	The Legal department manages all legal and regulatory matters and government relations, and it provides legal, strategic, and business advice to the Executive Management team and senior leadership of NSC. It also provides legal advice and guidance to the board of directors to ensure compliance with board and corporate governance policies. Legal advises NSC of changes in the law and the legal consequences of proposed actions. Legal engages in issues of data privacy and security to aid in ensuring proper departmental and organizational resources to facilitate compliance with laws, regulations, and best practices.
Education Solutions	The Education Solutions department oversees the successful formulation and execution of the mission, service delivery, and market strategies for institutional participation and revenue goals across the education community, which spans secondary, post-secondary, regional, and national education organizations. It identifies, develops, and onboards new business across the education community.

People	
Group/Role Name	**Function**
Business Solutions	Business Services serves current and former learners with better access to products, services, and employment opportunities by providing access to its academic achievement records. This is accomplished by improving access to commercial products and services by leveraging academic and credential attainment information. Business Services also protects students and alumni from identity fraud and synthetic ID fraud through seamless, real-time identity and age verification. It also enables alumni employment screening through certified degree verifications.
People Experience and Solutions	People Experience and Solutions is a collection of services that supports the primary internal business needs of NSC. These include, but are not limited to, Human Resources (HR) functions such as recruiting, onboarding, offboarding, associated policies, and managing training.
Enterprise Data Strategy and Governance	Enterprise Data Strategy and Governance focuses NSC's internal and external data strategies for scalability and effectiveness. This includes expanding the work with industry credentials, not-for-credit enrollments, and other credential providers, as well as connecting learners' experiences to labor outcomes.

The following NSC organization chart reflects the Company's internal structure related to the groups discussed above:



Procedures

Procedures include the automated and manual procedures involved in the operation of the VS and TS systems. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, IT, and HR. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of the VS and TS systems:

Procedures	
Procedure	**Description**
Logical and Physical Access	How the Company restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Mitigation	How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the application programming interface (API), the customer or end-user defines and controls the data they load into and store in the VS and TS systems production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks.

Data Input

Procedures and programs are in place to monitor processing integrity and to support the complete, accurate, and timely processing of customer transactions. Inputs are coded with unique identification numbers to enable them to be traced from initial input to output and from output to source inputs. Application edits limit the input to acceptable value ranges. Unacceptable inputs halt processing and raise errors to the Application Development team to resolve.

Data Processing

Once data is entered into the VS system, automated jobs transfer the data to the appropriate databases. Jobs do not store data within logs. If a job has an issue, an email is sent to the Application Production Support Group (APSG), where the issue is logged and addressed to completion.

A mirror image of application data files is replicated throughout the day to a second secure system for use in recovery and restoration in the event of a system disruption or outage. Application regression testing validates data processing within the application during the change management process. Transaction processing time is monitored for reasonableness.

Data Classification

Per the NSC Cybersecurity Policy, data is classified in one of three major categories: Public, Internal Use Only, and Confidential. Information classified as Confidential is private or otherwise sensitive in nature and restricted to those with a legitimate business need for access. Unauthorized disclosure of this information to people without a business need may be against laws and regulations, or may result in security breaches for NSC, its customers, or its business partners. Access provisioning is authorized by the data owner and, in certain cases, by NSC's Legal department.

Subservice Organizations

The Company uses subservice organizations for data center colocation services. The Company's controls related to the VS and TS systems cover only a portion of the overall internal control for each user entity of the VS and TS systems. The description does not extend to the colocation services for IT infrastructure provided by the subservice organizations.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. Controls are expected to be in place at the subservice organizations related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. The subservice organizations' physical security controls should mitigate the risk of unauthorized access to the hosting facilities. The subservice organizations' environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

The Company management receives and reviews the subservice organizations' SOC 2 or equivalent report annually. In addition, through its operational activities, Company management monitors the services performed by the subservice organizations to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreement; stay informed of changes planned at the hosting facilities; and relay any issues or concerns to management of the subservice organizations.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the VS and TS systems. Commitments are communicated in Customer Service Agreements and the Privacy Policy.

System requirements are specifications regarding how the VS and TS systems should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the VS and TS systems include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• The Company will employ reasonable security measures to protect confidential information. • The Company will maintain procedures and safeguards to limit physical access to confidential information and the facility or facilities in which it is housed while ensuring that only properly authorized access is allowed, including physical barriers that require keyed-entry or electronic control validation (e.g., card access systems) or validation by human security personnel. • The Company will maintain appropriate technical safeguards to ensure that personally identifiable information (PII) transmitted over an electronic communications network is not accessed by unauthorized persons or groups. • The Company will maintain ongoing security awareness through training or other means that provide its employees with updates to security policies and procedures, including guarding against, detecting, and reporting malicious software or activities. • In the event of an unauthorized or improper disclosure of customer information, the Company will promptly notify the customer of the incident, unless legally prohibited from doing so or specifically directed by law enforcement not to do so, within 72 hours after becoming aware of it.	• Management and business processes that include and enable security processes. • Ongoing personnel awareness of security issues. • Physical security requirements for information systems. • Governance processes for information technology (IT). • Reporting information security events and weaknesses. • Maintaining secure authentication protocols and access limitations for external and internal users. • Deploying network perimeter and other controls that ensure security from external threats. • Monitoring security information and event management (SIEM) and intrusion detection or prevention systems (IDS/IPS) 24/7. • Policies and procedures that maintain data security through all stages of the development life cycle.

Trust Services Category	Service Commitments	System Requirements
Availability	• The Company will back up all education record submissions from the institutions daily at an off-site facility subject to the Company's disaster recovery (DR) plan.	• Dedicated environmental controls, backup power systems, backup communication, and redundancy in network and IT systems. • Dedicated DR site and a tested DR plan and business continuity plan (BCP).
Processing Integrity	• The Company will maintain a detailed record of each verification request that is attempted or completed in a request record and make the request record available to the pertinent educational institution or its designated agent for review. • The Company will provide a timely response to each verification request based exclusively on data provided by participating educational institutions.	• Data input and data processing validations and procedures.
Confidentiality	• The Company will not disclose or transfer any confidential information to any third party, unless the third party is required to receive the confidential information to perform its services. • Upon expiration or termination of the services, and at the written request of the customer at any time, the Company will turn over to the disclosing party or destroy all confidential information in its possession.	• Dedicated privacy officer, Privacy Policy, data handling procedures, data loss prevention, and staff training. • FERPA regulations. • Data retention and destruction processes.
Privacy	• The Company will protect personal information in accordance with its Privacy Policy and the applicable FERPA requirements. • The Company will obtain consent for additional uses of PII collected directly from data subjects that are not described in its Privacy Policy. • The Company will respond to data access requests, including any denial of access to such requests, within 45 days.	• Dedicated privacy officer, Privacy Policy, FERPA staff training, and privacy program. • FERPA regulations. • Data subject request response system.