University Policy

Volume I1: Information Technology	I1.02.9 System and Organization Controls Reporting **Effective Date:** 06/30/2022 **Last Revised:** 05/30/2023	**Responsible Office:** University Technology Services
Chapter 02: Data Security		**Responsible Officer:** Chief Information Officer

POLICY STATEMENT

Northeastern Illinois University is committed to ensuring that the use of third-party systems and services does not expose the university to activities that could compromise the security of its information and operations. This is achieved through engaging third-party vendors that have risk-assessed their internal controls through independent audits and demonstrate that these controls adequately secure the IT services offered to clients, including the security and privacy of client data in their care.

PURPOSE OF THE POLICY

This policy sets out the requirements and procedure by which Northeastern Illinois University will verify and ensure that third-party service vendors demonstrate that internal controls exist and operate effectively to safeguard the security and privacy of university data. The aim is to ensure that the security of the university's information and operations are not undermined through the use of third-party systems and services.

WHO IS AFFECTED BY THIS POLICY

- All University End-user departments that use third-party systems and services to host, process, or manage university data.
- Third parties who provide IT systems and services to NEIU including infrastructure, software and cloud services to host and/or process university data.

DEFINITIONS

System and Organization Controls (SOC) Reports: As defined by the American Institute of Certified Public Accountants (AICPA), SOC reporting is the name of a suite of reports produced during an audit. It is intended for use by service organizations (for example, but not limited to organizations that provide information systems as a service to other organizations) to issue validated reports of internal controls over those information systems, in this example, to their clients. The reports focus on controls grouped into five categories called Trust Service Principles.

- SOC 1 – Designed for financial transaction processing. It is primarily used to validate controls over the completeness and accuracy of monetary transactions and financial statement reporting. Service organizations specify their own control objectives and control activities.
    - Type 1 – reports on the fairness of the presentation of management's description of the organization's system and the suitability of the design of the controls to achieve the related control objectives at a specific point in time.
    - Type 2 – reports on the fairness of the presentation of management's description of the organization's system and the suitability of the design of the controls to achieve the related control objectives over a period.

- SOC 2 – Designed to provide assurance over controls relevant to security, processing integrity, availability, confidentiality, and/or privacy of systems and the data the systems store or process. Service organizations are held to a standardized set of control criteria for each of the principles covered in their report. These reports can play an important role in the oversight of the organization, corporate governance, risk management processes, and regulatory matters.
    - Type 1 – reports on the fairness of the presentation of management's description of the organization's system and the suitability of the design of the controls to achieve the related control objectives at a specific point in time.
    - Type 2 – reports on the fairness of the presentation of management's description of the organization's system and the suitability of the design of the controls to achieve the related control objectives over a period.
- SOC 3 – This report covers the same testing procedures and requirements as a SOC 2 engagement, but the report omits the detailed test results and the description of the system and is intended for general audiences and public distribution.
- SOC for Cybersecurity – This report is designed to provide assurance about the effectiveness of the controls over a service organization's cybersecurity risk management program. An effective cybersecurity risk management program provides reasonable assurance that material breaches are prevented or detected, and mitigated in a timely manner.

Bridge Letter: A bridge letter, also known as a gap letter, is made available by a service organization to cover a period of time between the reporting period end date of the SOC report and the release of a new SOC report. This occurs because a SOC report covers only a portion of a fiscal year.

The bridge or gap letter can be used by the University as an interim assurance by management while waiting for the next SOC report. The bridge letter needs to be on file as part of the University's annual due diligence to show examiners that, as far as NEIU is aware, controls are still in place in between reports and that the service organization will provide the latest SOC reports as soon as they become available.

REGULATIONS

Use of third-party IT systems or services including cloud services must be authorized by University Technology Services before procurement. The use of such systems or services must comply with the university's Information Technology and Security Policies.

Since Northeastern Illinois University is regulated by State and Federal laws, it is imperative to ask existing as well as potential vendors to provide SOC reports as these have become essential for those vendors who handle critical information, systems or services on behalf of the University. SOC reports are essential to:

- Ensure that third-party vendors have carried out independent audits or testing of their internal controls.
- Verify that third-party vendors have sufficient controls in place to protect clients' information and critical operations, and the controls operate effectively.
- Provide a method of continuous monitoring and assurance of third-party internal risks management processes and compliance with regulatory requirements.

Responsibility

University End-user departments and University Technology Services (UTS) are responsible for ensuring that third parties demonstrate assurance that they operate robust risk management and governance processes for the services they provide as follows:

- University End-user departments: Are to inform UTS of any purchases of a third-party IT system or service at the inception of a project, procurement or contract review; and obtain SOC reports or an attestation that these reports exist (whichever applies) from the third party.
- UTS: is responsible for reviewing third-party SOC reports and advising the End-user department if the SOC findings are satisfactory or not.

Where a third-party vendor is unable to provide a SOC report, the vendor must provide an independent audit report to demonstrate assurance that they operate and maintain internal controls to appropriately secure the services offered to clients.

PROCEDURES

The procedure below should be followed for requesting SOC reports:

	Action	Responsibility	Next Step	
Step 1	Determine if vendor hosts and/or processes data on behalf of the University	End-user department (UTS to provide guidance if needed)	If yes, go to step 2	If not, a SOC report is not required.
Step 2	Contact the Purchasing Department to determine if the vendor is new or already exists	End-user department	If the vendor is new, request an attestation that SOC reports exist during IFB/RFP (if applicable) OR request SOC reports during procurement discussion and submit reports to UTS.	If the vendor already exists, request SOC reports for review and submit reports to UTS
Step 3	Review SOC reports	UTS	Provide a report to the End-user department and advise if SOC findings are satisfactory or not.	
Step 4	If the vendor is selected to provide a service, ensure there is a requirement for an annual SOC report submission either in the contract or added as an addendum.	End-user department/Purchasing Department	Advise UTS if the contract has been agreed with the vendor. Submit SOC reports to UTS annually.	

Request for a Bridge or GAP Letter

A bridge or gap letter should be requested by the End-user department from the third party and submitted to UTS whilst awaiting a new SOC report from the third party.

GUIDELINES

- Annually, End-user departments are to request the relevant SOC reports from respective service providers.
- If applicable, a Bridge Letter should be requested to cover a period of time between the reporting period end date of the SOC report and the release of a new SOC report.

HISTORY

Draft created June 2022

AUTHOR REFERENCE

"System and Organization Controls: SOC Suite of Services". *AICPA. Retrieved 2020-09-14.* - *https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html*
"SOC 1 - SOC for Service Organizations: ICFR". *AICPA. Retrieved 2020-09-14.* - https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc1report.html
"SOC 2 - SOC for Service Organizations: Trust Services Criteria". *AICPA. Retrieved 2020-09-14.* - *https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html*
"SOC 3 - SOC for Service Organizations: Trust Services Criteria for General Use Report". *AICPA. Retrieved 2020-09-14.* - *https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc3report.html*

CONTACT INFORMATION

Please direct questions or concerns about this policy to:

Contact	Phone	Email
Help Desk	(773) 442-4374	helpdesk@neiu.edu

DISCLAIMER

The University reserves the right to modify or amend sections of this policy at any time at its sole discretion. This policy remains in effect until such time as the Responsible Officer calls for review. Requests for exception to any portion of this policy, but not to the policy statement, must be presented in writing to the Responsible Officer.