University Policy

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.

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 ex 450.1a-153(n)7211(t)5(s)-62(a)-11

- 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 -11( )5(i)1sk ay-11(a)-111This 2 11 Tf17350.4 3d 436.

System