1. INTRODUCTION
   a. PURPOSE

This document, the UNC System Office Vendor Evaluation Standard and Procedure, acts as a supplemental standard and procedure to the UNC System Office Finance Policy Manual and UNC Board of Governors policy 1400.2. Vendor protections for sensitive information (Level 3 in the UNC System Office Classification policy) must be considered before purchase and sharing of the sensitive information and periodically reassessed thereafter.

b. SCOPE OF APPLICABILITY

All UNC System Office employees and contractors

2. POLICY FOUNDATION

In the Purchasing section of the UNC System Office Finance Policy Manual, the subsection “Responsibility for University System Office - Purchased Goods, Services, and Equipment” Indicates (“page 75) that the University System Office department head is accountable for their department’s purchases, regardless of funding source.” Any department initiating or renewing a procurement that might allow access beyond System Office staff to Level 3 (sensitive) information as defined in the Data Classification, Storage and Sharing policy, must follow the Vendor Evaluation Standard and Procedure maintained by the UNC System Office Department of Information Technology (DoIT). Contact help@northcarolina.edu to submit your request for vendor review or with any questions regarding that Standard and Procedure and ask that your ticket be assigned to the Third Party Vendor Management (TPVM) queue.

a. STANDARD and PROCEDURE

If a vendor may, at any time in the course of association with the UNC System Office, access sensitive information, protections the vendor provides for sensitive information (Level 3 in the UNC System Office Classification policy) must be assessed prior to purchase and prior to sharing of sensitive information and periodically reassessed thereafter. Assessment of the vendor protections will be requested by the department.
head or their designee and completed by the DoIT Chief Information Security Officer or Chief Information Officer or their designee. The authorized DoIT employee may indicate in written form that the purchase may proceed due to sufficient protective controls. Alternatively, the DoIT employee may prepare a written risk analysis for a Data Owner or their designee to consider and approve or deny the opportunity to share the information with the vendor. Finally, the Risk Review Board (RRB) has the authority to approve risks independent of the above. Vendor provided protections for all Level 3 information to which the vendor has access must be reconsidered at each purchase and contract renewal and no less frequently than every 36 months. Each DoIT assessment of protections must be documented such that the documentation can be produced on request for each assessed vendor consistent with the UNC System Office Records Retention program.

b. EXCEPTIONS

The Senior Officer named under Board of Governors (BoG) policy 1400.2 may grant exceptions in writing. In addition, the RRB may grant exceptions; such exceptions will be reflected in approved RRB minutes.

3. RELATED EXTERNAL SOURCES

- Board of Governors policy 1400.2

4. CONTACT INFORMATION

Primary Contact

Unit: Department of Information Technology

Email: help@northcarolina.edu

END of Standard and Procedure