Procurement Process Guidance
Annual Software Technologies, Applications, and/or Services Renewals

**Purpose:** To provide clear direction during the renewal process for any software based technologies, applications and/or services (“Technologies”) meeting one or more of the criteria specified in Old Dominion University (“University”) Policy 3509 to promote continued compliance with University Policy 3504 Data Administration Policy.

**Background:** University Policy 3509 provides guidance ensuring that any and all software based technologies, applications and services meet University information technology requirements and are compatible with existing technology standards and services.

University Policy 3504 establishes the framework for administering the University’s institutional data, including PII data, and provides guidance on the roles and responsibilities of data owners, security administrators, and system owners.

**Definitions:**

a. **Data Classification** - In the context of information security, it is the classification of data based on its level of sensitivity and the impact to the University should that data be disclosed, altered or destroyed without authorization.

b. **Data Element** - In electronic recordkeeping, a combination of characters or bytes referring to one separate item of information such as name, address, or age.

c. **Data Owners** - University employees (typically at the level of Registrar or Unit Director) who oversee data management functions related to the capture, maintenance, and dissemination of data for a particular operational area. They are responsible for decisions about the usage of institutional data under their purview.

d. **Data Users** - Those authorized to access institutional data and information in order to perform their assigned duties or to fulfill their role in the University community.

e. **Information Security Officer (ISO)** - The Old Dominion University employee, appointed by the President or designee, who is responsible for developing and managing Old Dominion University's information technology (IT) security program.

f. **Institutional Data** - Recorded information that documents a transaction or activity by or with any appointed board member, officer, or employee of the University. Regardless of physical form or characteristic, the recorded information is an institutional record if it is produced, collected, received or retained in pursuance of law or in connection with the transaction of University business. The medium upon which such information is recorded has no bearing on the determination of whether the recording is an institutional record. Institutional records include but are not limited to: personnel records, student records, academic records, financial records, patient records and administrative records. Record formats/media include but are not limited to email, electronic databases, electronic files, paper, audio, video and images.
g. **System Owners** - Managers responsible for the operation and maintenance of a University IT system or department heads responsible for overseeing hosted systems under their purview.

**Renewal Process:**

1. **Application:** This renewal process shall apply to all users of University Technologies either owned by or operated for University business through various contractual agreements.

2. **Procurement Services:**
   a. Prior to the execution of any renewal for Technologies, as described herein, Procurement Services shall facilitate communication between the System Owner and Information Technology Services to determine if the appropriate ITS Security Review and documentation have been completed;
   b. If the appropriate ITS documentation is in place, Procurement Services shall communicate with the System Owner, as described below;
   c. If the appropriate ITS documentation is not in place, Procurement Services shall communicate with both ITS and the System Owner to facilitate appropriate ITS documentation.
   d. Though Procurement Services will assist in the renewal process, it shall remain the System Owner's responsibility to initiate and complete the required ITS reviews and associated documentation.

3. **System Owner:**
   a. Prior to execution of any renewal of the University Technologies, the System Owner shall provide to Procurement Services for review and approval the Contractor's renewal proposal, which shall include:
      i. Scope of services;
      ii. Contract renewal term dates;
      iii. Any associated Terms and Conditions, EULA's, etc.; and
      iv. Pricing structure
   b. Prior to the execution of any renewal, the System Owner shall confirm to Procurement Services that (i) the data hasn't changed, (ii) no additional functionality has been added to the Technologies, and (iii) the System Owner still requires access to the data granted by the Data Owner.
   c. When applicable, if any changes to the data, use of data and/or system(s) necessitate a new and/or modified ITS Security Review, the System Owner shall be responsible for coordinating same with ITS.
   d. Otherwise, any existing Hosted Technology Addendum Form, when applicable, for the associated Technologies shall remain in effect during the renewal term by incorporating same by reference in the renewal agreement.

4. If the requirements for a requested renewal as stated herein can't be met, Procurement Services may deem the renewal request to be a “new” contract agreement versus a continuation of services, and may require that the applicable System Owner start anew by first having the ITS review(s) and associated documentation completed concurrently with Procurement Services' review of the contract agreement renewal.

5. Procurement Services may continue with renewals for existing services in order to maintain availability of services, in collaboration with IT Security. If a review is not possible prior to renewal, a Software Decision Analysis or System Risk Assessment will be scheduled with the System Owner as soon as is practical.