****

**Information Technology Security**

All Texas State University personnel are responsible for understanding when IT Security should be engaged for projects, new or existing service related tasks, and investigations.  IT Security can assist with security related issues such as requirement planning, defining scope, security design requirements, defining and reviewing Service Level Agreements (SLAs), designing and/or configuring security controls (detective, preventative, and corrective), evaluating third-party vendor policies and control documentation, performing research on regulatory compliance authorities, and assisting with risk management.

Texas State University IT Security should be engaged during the initial design of any new service, server, or application that will be used by University Staff, Faculty, or Students. The product selection stage of a project is the ideal phase to include IT Security and will ensure the product meets federal, state, and university security requirements. This allows for security methodologies to be part of the initial design and planning, rather than an afterthought during the conclusion of the project. Following this process will increase the chances that a proposed product or solution can successfully meet requirements, and subsequently be approved for use.

Please use the questions below to help identify indicators of risk during your evaluation phase. The Texas State IT Security team encourages you to fill this form out and provide it in an email to itsecurity@txstate.edu for all information system, services, or product explorations. Consistent with **UPPS 04.01.01 §03.02,** all information resources are required to be included in the risk assessment process and include vulnerability assessment prior to service launch.

Questions pertaining to the prospective service or application:

Is it hosted off-site (cloud)?     [X ] YES         [ ]  NO

Is there a similar service/application available used on campus? [ ] YES         [X ]  NO

Does this service need to be available off campus? [ X] YES         [ ]  NO

Is it part of or related to a grant?     [ ] YES         [ X]  NO

Do users login with a non-Txstate NetID account?      [ ] YES         [ X ]  NO

Are requirements regarding data retentions defined?    [ ] YES         [ X ]  NO

Does the service or application store or transmit any of the following data types?

Credit card or other payment data     [ ] YES         [ x ]  NO

Student records or information     [ ] YES         [ x ]  NO

Health records or information     [ ] YES         [ x ]  NO

Social Security Numbers     [ ] YES         [ x ]  NO

Personally Identifiable Information (e.g., DOB, Address) [ ] YES         [x ]  NO

Other regulatory data drivers/entities?     [ ] YES         [ x ]  NO

If you answered yes to any of the previous, please contact IT Security (itsecurity@txstate.edu)