

## **CEHD Information Security Procedure IS -2 Annual Risk Assessment**

In compliance to TAMU SAP 29..01.03.M0.01 (2.5, 3.1, 3.2), an annual Risk Assessment will be conducted for all Information Resources by the CEHD Information Security Officer or other designated personnel. This assessment will be based on state and university rules and SAPs as well as the Texas A&M Security Control Catalog and is done in compliance with Security Control Catalog RA-3. This assessment will be submitted to the Office of Information Technology Risk Management of Texas A&M University (ITRM) through Texas's Risk Assessment portal (SPECTRIM) or as otherwise directed by the Texas A&M CISO.

### **Non-Technology Services Administrators**

All approved non-Technology Services administrators are required to complete a Risk Assessment for the Information Resources they administer. The completed assessment must be transmitted to the CEHD ISO by March 1 of each year. The ISO will review, compile, and present these assessments to the CEHD Dean for approval. Failure to comply with this procedure may result in the loss of administrative access.

### **Alternate Assessor**

For larger IT projects, the project director may request the appointment of an alternate assessor to prepare and submit the Risk Assessment to ITRM. This request must be approved by the CEHD Dean and the ITRM. If approved, the project administrator will attend a training session by the ITRM and will work with the CEHD ISO to make sure the project risk assessment is submitted. Once submitted, the assessment must be approved by CEHD, ITRM, and the CISO.

Approved By: \_\_\_\_\_ Date: \_\_\_\_\_