FLORIDA	**OFFICIAL**
POLYTECHNIC	**TECHNOLOGY SERVICES**
UNIVERSITY	**STANDARD**

Subject/Title: Technology Services Risk Management Standard
Date Last Revised: 2020.01.28
Responsible Division/Department: Technology Services
Initiating Authority: Ben Beachy, Chief Information Officer

STANDARD OWNER

This standard is owned by the University Chief Information Officer.

STANDARD PURPOSE

This standard is to ensure that risks to the confidentiality, integrity, and availability of University information technology systems are appropriately assessed and that necessary corrective responses are made. This standard describes expectations for University employees and contractors.

STANDARD SCOPE

This standard applies to all information systems used for official University business. An information technology system is a combination of software, hardware, storage, telecommunication, and/or automated processes that generate value for the University.

Risk assessment requires close collaboration between:

- Technology Services staff; and
- The system owner(s)—staff member(s) with direct management control over the operations of the system.

STANDARD CONTEXT

Florida State law and FPU-1.0123P – University Public Records require that most University records be made available to public inspection. This legal requirement effectively dispenses with concerns for the confidentiality of public University records. Integrity and availability remain pertinent concerns, however; as does the confidentiality of those few records exempted from public disclosure. The requirements of this standard reflect this regulatory context.

STANDARD REVIEW

This standard must be reviewed at least once annually by the standard owner. It may be modified at any time by the standard owner. Any changes to this standard will be promptly reviewed with affected employees.

STANDARD

Risk assessment requirements

Technology Services' staff and systems owner(s) performing system risk assessment:

Must assess intrinsic risk. Intrinsic risk is present in the system before responses—mitigation, transference, or avoidance—are taken into account.

Must assess the intrinsic risks associated with:

- the confidentiality of system data;
- the integrity of system data; and
- the availability of system data.

Must include in their assessment:

- the inherent likelihood or probability of given risks; and
- the inherent scope or impact of those risks.

Must establish through their assessment:

- the classification of data in the system (reference FPU-11.00122P – University Data Classification and Protection)

Must identify responses to that reduce the intrinsic risk to an acceptably low level—that is, to a low level that University management can accept. The University does not accept high or moderate information security risks.

Risk assessment frequency

Technology Services staff and systems owner(s) must assess the information security risk of all systems prior to their procurement.

Technology Services staff must reassess risk at an interval determined by the assessed intrinsic risk of the system:

- Systems with high intrinsic risk must be reassessed no less than every six months.
- Systems with moderate intrinsic risk must be reassessed no less than every twelve months.
- Systems with low intrinsic risk must be reassessed no less than every twenty-four months.

Technology Services staff must also reassess system risk whenever significant changes are made to the system and/or its operating environment. Such reassessment may take the place of an interval reassessment.

Risk assessment documentation

Technology Services staff and systems owner(s) performing system risk assessment must document their work in an approved system. At a minimum, such documentation should include:

- The system being assessed.
- The person(s) performing the assessment.

- The date of the assessment.
- The date of the last assessment, if relevant.
- Assessment of the intrinsic risk to confidentiality, integrity, and availability.
- Classification of data
- Description of responses needed to make the risk acceptably low.
- The system owner(s)' acceptance of the responses and risks.
- The date of the next assessment based on the intrinsic risk of the system.

This documentation must be made available upon request to the Committee on Information Systems (COIS) as defined in FPU-11.00122P – University Data Classification and Protection.

All risk assessment documents are highly restricted data as defined in the University Data Classification and Protection Standard and are confidential information documents, not subject to disclosure under Florida State law and the University Public Records Standard FPU-1.0123P.

CHANGES

2019.12.24 Ben Beachy. First version.

2020.01.28 Ben Beachy. Terminological and typographic fixes.