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

Subject/Title: Technology Services Change Management Standard
Date Last Revised: 2019.12.24
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 changes to University systems are managed to reduce risks to the confidentiality, integrity, and availability of University information technology systems. 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. Changes to data alone are not in the scope of this standard.

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

All University systems must employ change management processes consistent with their intrinsic information security risk as determined in the Technology Services risk management procedures.

Change procedures

Systems with high intrinsic risk

Systems with high intrinsic risk must have a formal, documented change management procedure that includes documented management and, where appropriate, stakeholder approval of:

- Person(s) initiating the change
- Date of the change request
- Description of the change
- Business justification for the change
- Stakeholders affected by the change
- Information security impact
- Communication plan
- Testing plan
- Rollback plan

All changes to the systems with high intrinsic risk must be tested before deployment through sandboxes, test servers, or the equivalent.

All changes to systems with high intrinsic risk must be deployed in a manner that allows rapid, complete back-off through reversion functionality, snapshot restore, or equivalent.

Change management logs must be kept for systems with high intrinsic risk and must record the information above and:

- Person(s) implementing the change
- Date of change implementation
- Testing plan status: success or failure
- If testing failed, rollback status: success or failure

Systems with moderate intrinsic risk

Systems with moderate intrinsic risk must have a formal, documented change management procedure that includes documented management approval of:

- Person(s) requesting the change
- Date of the change request
- Description of the change
- Business justification for the change
- Stakeholders affected by the change
- Communication plan
- Testing plan
- Rollback plan

Change management logs must be kept for systems with moderate intrinsic risk and must record the information above and:

- Person(s) implementing the change

- Date of change implementation
- Testing plan status: success or failure
- If testing failed, rollback status: success or failure

Systems with low intrinsic risk

Systems with low intrinsic risk should have a change management procedure that includes management approval of:

- Person(s) requesting the change
- Date of the change request
- Business justification for the change
- Description of the change

Change management logs should be kept for systems with low intrinsic risk and should record the information above and:

- Person(s) implementing the change
- Date of change implementation

Authorized personnel

In all cases, changes to systems must be made by only authorized employees, or by vendors governed by contract with the University.

Change management logs

Change management logs must be retained consistent with University document retention policies but for no less than seven years.

Change management logs are restricted information as defined in FPU-11.00122P – Data Classification and Protection and must be protected consistent with that policy.

CHANGES

2019.10.28. Ben Beachy. Edited *Policy Scope*, and added *Policy Context* and *Policy Approval* for consistency with other policies.

2019.12.24. Ben Beachy. Replaced ‘policy’ with ‘standard’ to clarify intent. Minor typographic corrections.