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

Subject/Title: Technology Services Obsolete System Standard
Date Last Revised: 2020.01.14
Responsible Division/Department: Technology Services
Initiating Authority: Ben Beachy, Chief Information Officer

STANDARD PURPOSE

This standard is to ensure that obsolete information technology systems used by University employees are appropriately managed to limit information security risk. This standard describes expectations for University employees and contractors.

STANDARD SCOPE

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

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 OWNER

This standard is owned by the University Chief Information Officer.

STANDARD

Security

Obsolete systems are those no longer supported by commercially or generally available means. These systems pose unique information security and operational challenges to the University.

Whenever practical, the University will promptly replace or upgrade obsolete systems. While the costs of replacement or upgrade may appear significant in the short term, the long-term costs associated with obsolete systems generally outweigh these immediate costs.

When upgrade or replacement is not practical, Technology Services will work with system stakeholders to implement responses to the information security risk. Such responses may include:

- Removing the system from the network.
- Restricting the system to an isolated, secured network segment, VLAN, VRF, or equivalent.
- Restricting the system's access to the internet and/or other networks.
- Disabling or restricting the functionality of the system.

Periodic re-evaluation of responses to information security risk will be performed consistent with the Technology Services Risk Management Standard.

Exceptions to this standard must be be documented on the University Policy Exception Form and retained consistent with University practices.

Support

In all cases support for obsolete systems will be on a reasonable-effort basis. Technology Services does not guarantee the functionality or performance of obsolete systems.

Obsolete systems face greater than normal risk of failure at any time. Users of such systems should take special care to back up data and to maintain contingency plans. Technology Services does not guarantee the availability or integrity of data stored in obsolete systems.

Change management

Technology Services does not consider obsolete systems when assessing the impact of systems changes.

CHANGES

2020.01.14 Ben Beachy. First version.