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

Subject/Title: Technology Services Data Security 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 complements the FPU-11.00122P – Data Classification and Protection Standard and the FPU-1.0122P –Record Retention Standard to ensure that devices used for official University business are appropriately secured to limit information security risk.

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.

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

Data inventory

Technology services staff must maintain a University-wide inventory of information systems and must identify the data classification of each system as per FPU-11.00122P – Data

Classification and Protection. (As a matter of practice this work is combined information system risk assessment as per FPU-TS Risk Management Standard.)

Encryption

When encryption is required by University policy, Technology Services standard, or risk assessment, such encryption must use publicly-documented standards that have been evaluated by cryptography experts and are widely accepted within the industry; for example, the standards allowed in the National Institute of Standards and Technology (NIST) special publication 800-175B Guideline for using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms.

At rest

University data at rest must be encrypted when on devices not in physically secure areas. Secure areas include the University data center, contracted co-location space in other data centers, and other spaces with equivalent physical security.

To avoid any confusion, mobile devices storing University data at rest must be encrypted. For further details see FPU-TS Mobile Device Management Standards.

University data should be encrypted whenever practical when on devices in physical secure areas.

In motion

University data in motion must be encrypted when traveling within networks outside the University's direct control—through ownership or contractual arrangement. Information systems must be configured to enforce this requirement whenever possible.

To avoid any confusion, University data traveling over the internet must be encrypted.

University data in motion should be encrypted whenever practical when traveling within networks under the University's direct control. Information systems must be configured to enforce this requirement whenever practical.

Key management

Encryption keys are highly restricted data as defined in FPU-11.00122P – Data Classification and Protection. They must be given the highest level of protection available within the University.

Encryption keys must not be stored on the systems they protect.

Removable devices and removable media

Removable devices and removable media are included in the above encryption requirements for data at rest on devices not in physical secure areas.

To avoid any confusion, University employees are strongly discouraged from using removable devices and removable media. These devices are inherently unreliable and increase the risk of data loss and/or theft. University employees should instead store and access data within secure systems of record, or within secure network and/or cloud file storage systems.

If University employees must use removeable devices and removable media they must configure encryption in keeping with FPU-11.00122P – Data Classification and Protection and this standard. Technology Services provides documentation on encrypting removable media for supported operating systems:

- Data Encryption (Windows) – How to Encrypt Removable Media
- Data Encryption (macOS) – How to Encrypt Removable Media

Data controls

The following categories of data are defined in FPU-11.00122P – Data Classification and Protection:

Highly restricted data

Highly restricted data must be encrypted at rest and in motion.

Restricted data

Restricted data must be encrypted at rest and in motion when possible.

Unrestricted data

Unrestricted data should be encrypted at rest and in motion when practical.

Media destruction

Technology Services staff manage the destruction of all University-owned fixed and removable media. Such destruction must:

- Completely destroy the data through
    - physical destruction of the media (e.g. shredding);
    - physical destruction of data (e.g. magnetic degaussing);
    - and/or digital destruction of the data (e.g. overwriting data erasure).
- Be performed only by Technology Services staff or vendors approved by Technology Services and University Procurement.
- Certify chain of custody and destruction of data.

CHANGES

2019.12.24 Ben Beachy. Initial draft.

2020.01.28 Ben Beachy. Elaboration of standard requirements.