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

Subject/Title: FPU Technology Services Mobile Device 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 mobile devices used by University employees are appropriately managed to limit information security risk. This standard describes expectations for University employees and contractors.

University students and student-owned devices not used for official University business may be managed in accordance with this standard but are not required to be.

STANDARD SCOPE

This standard applies to all mobile devices 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. A mobile device is a laptop, smartphone, tablet, or similar device.

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

User responsibilities

Employees must be informed of their responsibilities regarding mobile devices and University data, and appropriate responses to the theft or loss of mobile devices. (As a matter of practice this may be managed by the University Human Resources department during employee orientation.)

Employees must sign the University Off-Campus Property Permit before taking possession of University-provisioned mobile devices. (As a matter of practice this may be managed by staff outside Technology Services.)

Employees must surrender University-provisioned devices upon the termination of employment. (As a matter of practice mobile device recovery may be managed an employee's supervisor and/or the University Human Resources department.)

Employees are responsible for maintaining the physical security and information security of mobile devices (including obligations for 'Device Management', below) and must report lost or stolen devices immediately to the University Information Security office by calling 863.874.8888 or emailing helpdesk@floridapoly.edu.

Device management

To ensure compliance with University policies and technology services standards, University-provisioned mobile devices must be managed using centralized tools; user-owned mobile devices used for official University business should be managed using centralized tools when practical.

Mobile devices, whether University-provisioned or user-owned, must be configured to:

- Automatically lock after no more than 15 minutes of inactivity.
- Require a five-character or longer PIN, strong password (See FPU-TS – Access Management Standard for further details on strong passwords), or biometric authentication to unlock.
- Authenticate against University-standard systems including single sign-on (SSO) and multi-factor authentication (MFA). (See FPU-TS – Access Management Standard for further details on SSO and MFA.)
- Require periodic re-authentication to connect to University systems. (See FPU-TS – Access Management Standard for further details on password reset frequency.)
- Encrypt all data on the device and any attached storage. (See FPU-TS – Data Security Standard for further details on encryption.)
- Wipe all University data on the device upon authorized remote command.

CHANGES

2019.12.24 Ben Beachy. First version.

2020.01.28 Ben Beachy. Clarified focus on University employees and University business, not student activity.