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

Subject/Title: Technology Services Access 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.

STANDARD SCOPE

All accounts 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

User Responsibilities

Users are responsible for activity originating from their account that is reasonably within their control.

Users are responsible for keeping their University accounts and passwords secure and may not share their University accounts or passwords with others.

Users must immediately report security breaches concerning to their account to the University Information Security office by calling 863.874.8888 or emailing helpdesk@floridapoly.edu. The University will not retaliate against an individual reporting an observed or suspected security breach.

Users may not use automatic login provisions of web browsers or similar applications.

Authorization

Access to University systems must take place through accounts managed by Technology Services. Accounts must not be provided for employees until authorization is received from University Human Resources; accounts must not be provided for contractors until authorization is received from University Procurement.

Access to University systems beyond that granted to the general public must not be granted without approval from a manager or supervisor, except that access to systems available to all University employees may be granted upon account creation.

All access to University systems beyond that granted to the general public must be logged in accordance with FPU-TS Logging and Monitoring Standard.

Accounts must be suspended upon notification from Human Resources, or the contract sponsor, or upon contract termination.

Passwords

Passwords for user accounts must be changed at least every 180 calendar days. Passwords for user accounts must not be able to change more often than every 5 calendar days, unless overridden by an authorized administrator.

Passwords for user accounts must not be re-used. The password management system must include a password history of at least twelve previously used passwords and prevent their re-use.

The University's password management system must enforce the following constraints:

- Passwords must be changed at least every 180 calendar days.
- Passwords may not be changed more often than every 5 calendar days.
- At least twelve previously used passwords must be stored and reuse of these passwords must be prevented.
- Passwords be at least eight characters in length and must meet complexity requirements as defined by Microsoft at https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements[1].

[1] "1. Passwords may not contain the user's samAccountName (Account Name) value or entire displayName (Full Name value). Both checks are not case sensitive….
"2. The password contains characters from three of the following categories:

- "Uppercase letters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)

User accounts must be locked after no more than five failed logins and must remain locked for at least thirty minutes.

Multi-factor authentication (MFA)

University information systems must be configured to use multi-factor authentication where practical.

Users should access multi-factor authentication codes through smartphone applications or hardware tokens; phone calls and text messages, while supported, are discouraged as less-secure alternatives.

Multi-factor authentication codes should be changed no less than every two minutes.

Single sign-on (SSO)

University information systems must be configured to use the University's AD-FS single sign-on system where possible. Exceptions will be noted as part of risk management processes (see FPU-TS Risk Management Standard for details.)

CHANGES

2019.12.24 Ben Beachy. First version.

2020.01.28 Ben Beachy. Clarification of language. Elaboration of MFA and SSO requirements.

- "Lowercase letters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
- "Base 10 digits (0 through 9)
- "Non-alphanumeric characters (special characters): (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/) Currency symbols such as the Euro or British Pound are not counted as special characters for this policy setting.
- "Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages."

Retrieved from https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements on 2019.12.24.