Information Technology Policy

9.2000

Document Review Log

Date Reviewed	Description of Changes
8/17/2023	Initial Draft approved by Senior Leadership Team

Consent to Monitoring/ No Expectation of Privacy

End users, including faculty, staff

1.

g) Shall immediately report loss of any device used to access AU systems or data to the AU. This will allow the Help Desk to remotely remove any Mobile Device Management software that may have been installed.

h) Shall (y)-4.5148042ifyvs

Passwords

Access to computers, software applications and electronic information is frequently password controlled. Users are responsible for creating and protecting passwords that grant them access to resources. Passwords cannot be shared, displayed in plain view, or stored in computers.

Passwords used to access systems must meet password length, complexity, and longevity requirements. Although different systems may have unique password requirements, all passwords must be a minimum of 12 characters long, and must contain at least one of each of the following:

- Upper case letter (A-Z)
- Lower case letters (a-z)
- Numbers (0-9)
- Special characters (e.g. !, #, &, %, extended ASCII, etc.)

Passwords should not contain names or permutations of personal data such as social security numbers, dates of birth, etc. Default passwords must be changed on a user’s first login. Generally, systems will enforce the timeframe when passwords must be changed (usually every 180 days). Use of a password vault is recommended.

Computer Security

Users must take steps to protect their desktop, laptop, and mobile devices from compromise either by the public or members of the AU

Consequences of Not Complying with this Policy

The greatest consequence of end user non-compliance of this policy is that it will put AU systems and data at risk. In addition, end users may be subject to disciplinary acti s,sdt andancandanteNmanati s employm ent9.2.4 ( )10.6U(i)-3.3 (n)-0.7l(a)-

Exhibit A –

x	Injury and Illness Incident Reports (OSHA Form 301) and related Annual Summaries (OSHA Form 300A); Logs of work-related injuries and illnesses (OSHA Form 300)	7 years following the end of the calendar year that these records cover	Keep health, medical and safety data