ITS POLICIES AND GUIDELINES
CATEGORY: Information Technology, Security, Information Access & Management
STATUS: Interim Approved

POLICY TITLE: **Mobile Device Security Policy**

POLICY PURPOSE:
The Data Security Policy defines the roles and responsibilities for creating, accessing, transmitting and storing University data. This policy defines the additional requirements for handling university data on mobile devices.

APPLIES TO:
This policy applies to anyone with access to Truman data, systems or networks. It includes all Truman faculty, staff, students, contractors, consultants, temporary employees, and all personnel with access to Truman data.

CONTENTS:

POLICY STATEMENT:

A mobile device is a small handheld computing device, typically having a display screen with touch input and/or a miniature keyboard. It has an operating system (OS), application software packages and storage for data. The mobile device may have wireless connectivity capabilities such as Wi-FI, Bluetooth, radio frequency identification (RFID) or cellular service. Examples of mobile devices are: personal data assistants (PDAs), smartphones, Blackberrys, Apple iPads, tablets, notebook or laptop computers etc.

As defined in the Data Security Policy, "All members of the University community have a responsibility to protect the confidentiality, integrity, and availability of any data that is created, accessed, modified, transmitted, stored or used by the University, irrespective of the medium on which the data resides and regardless of the format (such as electronic, paper or other physical form)."

The Data Security Policy classifies University data as follows:

Level I – Confidential Information
Level II – Sensitive Information
Level III – Public Information
Level IV – Proprietary Information

All mobile devices handling University data other than Level III (public information) must use appropriate security measures to ensure University data is protected from unauthorized physical or wireless access. This should include but is not limited to: A mobile device logon userid or PIN, encryption of the storage media and restricting wireless access. The mobile device logon credentials and encryption keys for storage media must be provided to ITS for secure storage.

EXCLUSIONS OR SPECIAL CIRCUMSTANCES:
Any exceptions to this policy must be approved in writing by ITS (see contact information below).

CONSEQUENCES:
By failing to abide by this policy or policy procedures, individuals may be subject to sanctions, up to and including the loss of computer or network privileges, disciplinary action, suspension, termination of employment, dismissal from the University, and legal action. Some violations may constitute criminal offenses under local, state, and federal laws. The University will carry out its responsibility to report such violations to the appropriate authorities.

CONTACTS:

Responsible Executive:	Provost and Vice President for Academic Affairs
Responsible Office:	Information Technology Services
Contact:	Chief Information Officer 111 McClain 660-785-4163
APPROVED BY:	President, Truman State University
APPROVED ON:	2020/04/01
EFFECTIVE ON:	2020/04/01
REVIEW/CHANGE HISTORY:	
REVIEW CYCLE:	As Needed

DEFINITIONS:

ITS – Information Technology Services
OS – Operating System
PDA – Personal Data Assistant
PIN – Personal Identification Number
RFID – Radio Frequency Identification
USERID – User Identification

RELATED DOCUMENTS:

KEYWORDS: