Information Technology Executive Council (ITEC)

ITEC 7030-P

1.0 TITLE: Mobile Device Policy

2.0 PURPOSE: This policy establishes specific security requirements for Mobile Devices.

3.0 SCOPE: This policy applies to all Mobile Devices owned or leased by the Entity.

4.0 ORGANIZATIONS AFFECTED: This policy applies to all State of Kansas branches, boards, commissions, departments, divisions, Entities, and third parties involved in processing, transmitting, or providing business capabilities on behalf of Kansas state government, hereafter referred to as Entities.

5.0 REFERENCES:

5.1 National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, as amended

5.2 NIST Special Publication (SP) 800-53 Revision 5, as amended

6.0 DEFINITIONS:

6.1 Mobile Devices (or devices): Include items such as smartphones, tablets, and e-readers.

6.2 Mobile Device Management (MDM): The administration of Mobile Devices typically implemented through a third-party product with management features for Mobile Devices.

7.0 POLICY: This policy governs mobile device security. Entities may impose supplemental restrictions through specific policies, but such policies must not contradict the provisions outlined here.

Entities must:

Mobile Device Hardening

7.1 Where possible, centralize control of Mobile Devices through MDM or a similar centralized management system.

7.2 Configure Mobile Devices according to current and applicable CIS Benchmarks.

7.3 Erase or render the data on Mobile Devices inaccessible after no more than 6 consecutive failed login attempts.

7.4 Configure Mobile Devices to automatically lock after 2 minutes or less of inactivity.

Mobile Device Approved Application Stores

7.5 Establish, maintain, and disseminate a documented list of approved applications stores through which Mobile Devices may obtain Entity approved applications.

Mobile Device Approved Applications

7.6 Establish, maintain, and disseminate a documented list of approved applications authorized for installation and use on Entity issued Mobile Devices for official business purposes.

7.7 Restrict installation and use of mobile applications on Entity issued Mobile Devices not supported by a documented and approved business justification.

Mobile Device Application Management

7.8 Ensure all applications and operating systems on Entity issued Mobile Devices are updated to the latest vendor-supported version.

Mobile Device Approved Cloud Services

7.9 Establish, maintain, and disseminate a documented list of approved cloud services for use with Mobile Devices for Entity business purposes.

7.10 Restrict the use of personal email accounts, personal storage accounts, and other personal cloud services on Entity issued Mobile Devices not supported by a documented and approved business justification.

Mobile Device Backup

7.11 Prohibit backing up Entity information from Entity issued Mobile Devices to personal computers, personal storage devices, and personal cloud services.

8.0 RESPONSIBILITIES:

8.1 Heads of Entities must establish procedures to ensure compliance with this policy.

8.2 The Chief Information Security Officer (CISO), Executive Branch, is responsible for maintaining this policy.

9.0 ENFORCEMENT:

9.1 Non-compliance with this policy may result in disciplinary action, including termination of employment for severe violations.

9.2 Written approval from the Kansas Information Security Office (KISO) is required for any exception to this policy.

10.0 CANCELLATION: This policy cancels and supersedes all previous versions.