The University of Texas
Rio Grande Valley
Information Security Office

# Data Protection Standard for Personally Owned Mobile Devices

## 1. Purpose

These minimum standards serve as a supplement to the UTRGV Computer Security Standard, which was drafted in response to UTS-165. Adherence to the standards will increase the security of Mobile Devices and help safeguard UTRGV information resources. These minimum standards exist in addition to all other UTRGV policies and federal and state regulations governing the protection of UTRGV's data.

## 2. Scope

This standard applies to all personally owned Mobile Devices which access or store UTRGV data.

## 3. Audience

All employees, students, consultants, vendors, contractors, and others who own or operates a Mobile Device which stores or accesses UTRGV data.

## 4. Authority

UTS 165, UTRGV AUP

## 5. Definitions

**Mobile Device** – includes but is not limited to all tablets, mobile phones and similar devices.

**Personally Owned** – includes any Mobile Device which is not owned, leased or managed by UTRGV.

## 6. Standard Details

**All Mobile Devices which access UTRGV information resources:**

6.1 Must be password protected in accordance with UTRGV requirements, and passwords must be changed whenever there is suspicion that the password has been compromised.

**Additionally, all Mobile Devices which access and store UTRGV data, including UTRGV email:**

6.2 Must be a fully vendor supported device.

6.2.1 Jailbroken, rooted or similarly modified Mobile Devices are not authorized.

6.3 Operating system and application security updates and/or patches must be expediently installed.

6.4 Must be free of malware and not using software in a manner that infringes on copyright laws.

6.5 Must be encrypted using methods approved by the Information Security Office.

6.6 Must be configured to auto-lock and password protect after 5 minutes of inactivity.

6.7 Must have an auditing tool that allows the Information Security Office to validate the Mobile Device is compliant with this standard.

6.8 Mobile Device backups must be password protected and encrypted using methods approved by the Information Security Office.

6.9 Confidential UTRGV data created and/or stored on a Mobile Device should be transferred to UTRGV owned or sanctioned storage as soon as feasible.

6.10 Mobile Devices that are lost or stolen must be immediately reported to the Information Security Office.

6.11 Mobile Devices are subject to Public Information Requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to University Information Resources.

## 7. Roles and Responsibilities

**End User**: Ensures that the Mobile Device that they own or operate meets this security standard. Engage with UTRGV Computer Support Staff for guidance and compliance with this standard.

**UTRGV Computer Support Staff**: Ensure that all Mobile Devices which store or access UTRGV data are configured to support the minimum requirements as defined in this standard.

**Information Security Office**: Define and maintain this standard to a level that can define necessary configurations and security practices to protect UTRGV information resources and ensure compliance with all UT System, state and federal policies and standards.

## 8. Non-Compliance and Exceptions

Mobile Devices which do not adhere to the minimum requirements defined in this standard or otherwise pose a threat to UTRGV Information Resources may have their access to UTRGV information resources immediately revoked without notice.

## 9. Related Policies, Standards and Guidelines

UTS 165
UTRGV AUP
UTRGV Computer Security Standard

## 10. Revision History

| Version | Date | New | Original |
|---|---|---|---|
| 1.0 | 05/05/2016 | Standard Created | N/A |
| 2.0 | 10/09/2017 | Standard updated to clarify the requirements of devices when they only access UTRGV data vs when they both access and store UTRGV data. | |