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 store or access UTRGV data.

3. Audience
All employees, students, consultants, vendors, contractors, and others who own or operate 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
6.1. Must be a fully vendor supported device.
6.1.1. Jailbroken, rooted or similarly modified Mobile Devices are not authorized.
6.2. Operating system and application security updates and/or patches must be expediently installed.
6.3. Must be free of malware and not using software in a manner that infringes on copyright laws.
6.4. Must be password protected and encrypted using methods approved by the Information Security Office.
6.5. Must be configured to auto-lock and password protect after 5 minutes of inactivity.
6.6. Must have an auditing tool that allows the Information Security Office to validate the Mobile Device is compliant with this standard.
6.7. Mobile Device backups should only be stored on UTRGV owned or sanctioned storage and must be encrypted and password protected.
6.8. Mobile Devices that are lost or stolen must be immediately reported to the Information Security Office.
6.9. 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

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>New</th>
<th>Original</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>05/05/2016</td>
<td>Standard Created</td>
<td>N/A</td>
</tr>
</tbody>
</table>