The University of Texas Rio Grande Valley
Information Security Office

Norma para protección de datos para dispositivos móviles personales

1. Propósito

Estas normas mínimas sirven como complemento a la Norma de Seguridad Computacional de UTRGV, que fue elaborada en respuesta a la UTS -165. El cumplimiento de las normas aumentará la seguridad de los dispositivos móviles y ayudara a proteger los recursos de UTRGV informáticos. Existen estas normas mínimas, además de todas las demás políticas de UTRGV y reglamentos federales y estatales que rigen la protección de los datos de UTRGV.

2. Alcance

Esta norma se aplica a todos los dispositivos móviles personales que almacenan o tienen acceso a datos de UTRGV.

3. Audiencia

Todos los empleados, estudiantes, consultores, proveedores, contratistas y otros que poseen u operan un dispositivo móvil que almacena o tiene acceso a datos de UTRGV.

4. Autoridad

UTS 165, UTRGV AUP

5. Definiciones

Dispositivo Móvil - incluye pero no se limita a todas las tabletas, teléfonos móviles y dispositivos similares.

Propiedad personal - incluye cualquier dispositivo móvil que no es propiedad, alquilado o administrado por UTRGV.

6. Detalles de la norma

6.1. Debe ser un dispositivo totalmente compatible vendedor.

6.1.1. Dispositivos móviles, con jailbroken, rooted o similarmente modificados no están autorizados.

6.2. Actualizaciones del sistema operativo y aplicaciones de seguridad y/o parches deben de ser instalados periódicamente.

6.3. Debe estar libre de malware y no usar el software de una manera que infrinja las leyes de copyright.

6.4. Deben ser protegidos con contraseña y encriptados usando métodos aprobados por la Oficina de Seguridad Informática.

6.5. Debe estar configurado para auto-bloqueo y proteger con contraseña después de 5 minutos de inactividad.

6.6. Debe tener una herramienta de auditoría que permita a la Oficina de Seguridad Informática para validar el dispositivo móvil es compatible con este estándar.

6.7. Copias de seguridad de dispositivos móviles sólo deben ser almacenadas en el almacenamiento de propiedad de UTRGV y deben estar cifradas y protegidas con contraseña.

6.8. Los dispositivos móviles que fueron perdidos o robados deben ser reportados inmediatamente a la Oficina de Seguridad Informática.

6.9. Los dispositivos móviles están sujetos a peticiones de información pública, mandatos, órdenes judiciales, solicitudes de descubrimiento y otros requisitos aplicables a los recursos de información de la Universidad.

7. Roles y Responsabilidades

Usuario final: asegura que el dispositivo móvil que posee u opera cumple con esta norma de seguridad. Compromete con UTRGV Soporte Técnico para su orientación y el cumplimiento de esta norma.

UTRGV Personal de soporte técnico: Asegura de que todos los dispositivos móviles que almacenan o tienen acceso a datos de UTRGV están configurados para admitir los requisitos mínimos definidos en esta norma.

Oficina de Seguridad Informática: Define y mantiene esta norma a un nivel que puede definir las configuraciones necesarias y prácticas de seguridad para proteger los recursos de información de UTRGV y garantiza el cumplimiento de todas las políticas y normas de UT System, estatales y federales.

8. Incumplimiento y Excepciones

Los dispositivos móviles que no se adhieren a los requisitos mínimos definidos en esta norma o que representen una amenaza para los recursos de información de UTRGV pueden tener su acceso a los recursos de información de UTRGV anulados inmediatamente sin previo aviso.

9. Pólizas, normas y consentimiento relacionados

UTS 165
UTRGV AUP
Norma de Seguridad Computacional de UTRGV

10. Historial de Revisión

Version	Date	New	Original
1.0	05/05/2016	Standard Created	N/A