PROPOSED POLICY

P02.07.066. Mobile Device Security Policy

University employees and students who use a laptop computer or mobile device (e.g. portable hard drives, USB flash drives, smartphones, tablets) are responsible for the university data stored, processed or transmitted via that computer or mobile device and for following the security requirements set forth in this policy and other applicable Information Resources Policies regardless of whether that device is the property of the university or the individual.

The use of unprotected mobile devices to access or store non-public information is prohibited regardless of whether or not such equipment is owned or managed by the university.

The Chief Information Technology Officer (CITO) is responsible for coordinating with the campuses in the development of consistent measures and business practices for ensuring the security of sensitive data on mobile devices.