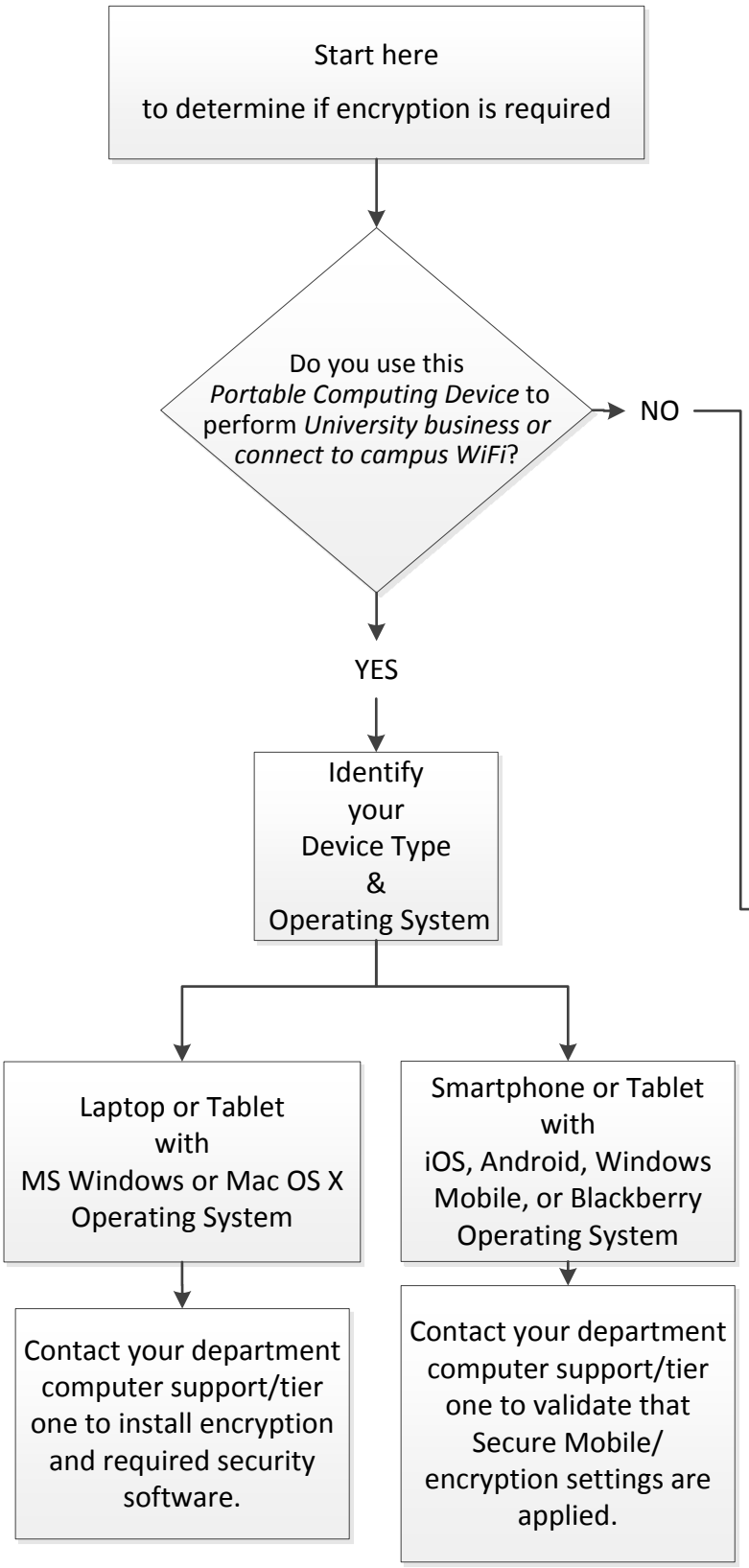
HEALTH SCIENCES CENTER

Portable Computing Device Encryption

Choose the right encryption solution for your device!



Portable Computing Device (PCD): includes but is not limited to notebook computers; tablet PCs; handheld devices such as Portable Digital Assistants (PDAs), iPads; iPods; smart phones such as iPhones, Androids, RIM (Blackberry) and MS Windows phones; and converged devices.

University business: work performed as part of your job responsibilities as an employee of the University, or work performed on behalf of the University as faculty, staff, volunteers, students and other trainees, and other persons whose conduct, in the performance of work for the University, is under the direct control of the University, whether or not they are paid by the University ("workforce"). In the context of laptop use, University business would include the use of a laptop to access non-public University systems, networks or data in the performance of work for the University.

Policy: All *Portable Computing Devices* (PCDs), irrespective of device ownership, that connect to non-public university information resources must follow University policies and standards for the security of these resources. This includes PCDs that access University email systems.

ALL laptops and mobile devices used for University business must be encrypted, regardless of who owns the laptop, or the operating system used.

http://it.ouhsc.edu/policies/