I. PURPOSE

The purpose of this standard is to establish a baseline for configuring smart phones and mobile storage devices that are used to collect, store, process or transmit confidential or sensitive University information assets – regardless if the devices are personally-owned or owned by the University.

Units may implement more restrictive controls and safeguards than those outlined herein; however, units implementing less restrictive controls and safeguards shall receive approval from the University Chief Information Security Officer (CISO) *before* the smart phones and mobile storage devices are implemented in production or approved for use in accessing University information assets.

- Exception requests shall be submitted to/through the UKAT Service Desk. The UKAT Service Desk will then assign and forward requests to the University CISO for disposition. If desired, dispositions can be appealed to the University Chief Information Officer (CIO).

Units implementing cyber security safeguards, policies and practices that are not explicitly addressed by this standard shall reference and implement the **SANS Critical Security Controls** and/or the **National Institute of Standards and Technology (NIST)** cyber security policies, procedures, standards and guidelines (i.e., http://csrc.nist.gov/publications/PubsTC.html, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.)

II. APPLICABILITY

This policy is applicable to all personnel who use smart phones and mobile storage devices to collect, store, process or transmit confidential or sensitive University information assets – regardless if the devices are personally-owned or owned by the University.

III. THE STANDARD

Smart phones, USB thumb drives, and cloud computing storage are all very useful tools for accessing email and transferring data between computers; however, these tools can be a liability if they are not managed appropriately.

1. **Review** UK Administrative Regulations and UKAT Policies, Procedures, Standards & Guidelines to ensure you are compliant with University policy and best practices.
2. **Password Protect It** – if you can. Almost all new smart phones support "login passwords"; however, some folks don't like the hassle of having to type or "swype" in their password before using the phone. If you ever lose your phone, you will be grateful for having setup a password.
3. **Encrypt It** – if you can. Many mobile devices support encryption. Many smart phones support the encryption of both the internal storage and removable storage chips. Such encryption rarely interferes with the device's/phone's operation and it will provide you with another layer of assurance if your device/phone is ever misplaced or stolen.
4. **Remote Wipe** – Many mobile devices also support the ability to erase the contents remotely (i.e., delete the contents from somewhere else, like from a laptop computer with Internet access

- if the device is ever lost or stolen.) This is another piece of security insurance. Most remote-wipe products require the owner to register well in advance of ever permitting someone to login and order a remote wiping of a smart phone's memory.

5. **Anti-Malware** – Many mobile devices also permit the installation of anti-virus or anti-malware software (or it may come with such software pre-installed.) Such software may scan applications that you try to install or scan email that you receive on your mobile device – looking for computer viruses, etc.. Read the fine print. Every piece of anti-malware software is different.

6. **Back It Up** – Many mobile devices support the "backing up" or copying of certain data to another location or another device so that, if your device gets stolen or lost or simply quits working properly, you will be able to restore the data but - be careful. Some back-up applications only make a copy of your phone's address book and others only make copies when you explicitly tell it to do so. Again, read the fine print. It is very prudent to make sure that the important data on your device is being backed up to a reputable location before you need to restore it.

7. **Buyer Beware** – More and more malicious software (aka "malware") is being embedded in mobile device applications. These applications, applets, or "apps" can often be downloaded from the Internet for free or shared by some other mobile device owner.

   Advice: After you research the application to learn what it does, what private data it wants/needs to run, how it supported, and how much it costs, research the website or application through which you are downloading the software. The application itself may be great but, if a cyber-crook creates another application that looks the same but contains dangerous or malicious software, you may regret buying or installing the app.

IV. DEFINITIONS *(not complete)*

V. REFERENCES

VI. REVISION HISTORY

Date	Description	Primary Author
12/18/14	Initial draft developed	M. Carr

VII. END NOTES