**PURPOSE:**

- To provide a policy to describe the current use of Personal Data Assistants (PDAs) and Smart Phone type equipment in the Division of Student Affairs.
- To ensure the security of the University / Division’s confidential data.

**SCOPE:**

The scope of this document is to define the secure use of Smart Device type equipment.

**POLICY:**

The use of handheld technology in today’s society is a fact of life. Protecting confidential data is also a fact of life in today’s society. Understanding both previous statements, the staff in the Division of Student Affairs has or will have the need to use some form of Smart Device now or in the future to keep them aware of a variety of tasks each day. The tasks may include checking calendars, e-mail, the WEB, and task list. When we use these devices for online tasks, they become just as vulnerable as our laptops / desktops workstations to viruses, exploits and many other threats. As with laptops, they also introduce another element. The additional element is THEFT. The theft of any of our devices introduces the risk of losing data. The data loss can range from personal data to confidential university data. During the holiday seasons, many staff members purchase the now famous “$79 computers” and are looking to have Student Affairs Information Technology (SAIT) install the new software without know the overall ramifications of using the device in our work environments.

Research shows that there are six (6) areas of concern when using Smart Devices:

1. Theft of the device (the biggest risk)
2. Viruses and data corruption (the second biggest risk)
3. Password theft
4. Data loss through line sniffing
5. Mobile code vulnerabilities
6. Wireless vulnerabilities (when used to surf the WEB)

Given the above threats, Student Affairs Information Technology and the Division of Student Affairs are sharing the following Security requirements relating to Smart Devices:

- All data on these devices must be encrypted.
- All data on these devices must be protected from virus threats
- Users must not use their devices to send or receive e-mails that contain private and sensitive information.
- All devices must be password protected and must support periodic password changes.
- All devices that are used to surf the internet, must use a virtual private network (VPN) client.

SAIT has identified the following devices that will be supported on the Division’s network in 2009 and 2010:

- Blackberry smart devices – Models will be determined by current available technology that will work in the Division’s environment.
- iPhones and similar devices.

  - NOTE: All devices require special permission of the Vice President of Student Affairs after recommendations from the Director of Student Affairs Information Technology.

Revision History:

- New January 2008 – JMoore
- Revised October 2009 – JMoore