# University of Dayton

# Guidance for Interpreting University-sponsored Purchases of iPads and Mobile Tablet Devices

*June 22, 2011*

## 1. Introduction

In an effort to better understand the role and value of iPads and similar mobile tablet devices in higher education, the University reviewed the following resources:

a) Educause Website and related materials
b) Campus technology Website and database
c) Gartner Database
d) Web search focusing on iPad initiatives and evaluations at universities and colleges
e) Web search focusing on universities/colleges purchase and use policies for iPads and similar devices[1]

Additionally, UDit's risk management unit analyzed the information security risks associated with these devices and has prepared an overview of security considerations and several recommendations for ensuring appropriately secure use of these devices as they currently are being used.

## 2. Context of Tablet Computing in Higher Education:

iPads and mobile tablet devices are emerging as valuable academic tools that can effectively support and enhance teaching, research, advising and related communication and collaboration activities. However, at this time, these devices will not replace the functionality of notebooks or desktop computers. ***The University of Dayton is not in a financial position to distribute these devices to all members of the faculty or staff while continuing to provide individuals with a relatively current notebook or desktop computer.*** Furthermore, the University must carefully adhere to IRS guidelines that require the University to account for "taxable benefits" for devices that may be used for personal purposes by employees.

Given the above stated conditions, tablet devices were specifically incorporated into the Policy on Computer Purchases.

## 3. Guidance on interpreting tablet computer purchases:

a) The request for permission to purchase an iPad or similar tablet device must be accompanied by a detailed rationale outlining the academic or business use of the device that demonstrates relevant need and institutional benefit. The rationale should be specific to the functionality of the device.

[1] See Appendix A for further discussion on iPad and Tablet devices in Higher Education

b) Purchases of "software applications" for these devices on University accounts must be accompanied by an explanation detailing the relevant academic or business need for the application.

c) In most cases, recurring service fees for connectivity will not be paid for by the University. These devices should be configured for Wi-Fi access. 3G or 4G access fees (or similar cellular connections) must be personally paid by the user unless specifically exempted by the Dean or Unit VP based on the documented academic or business rationale. If University-sponsored 3G or 4G access is approved, the service and billing must be coordinated through UDit.

d) Users of University-owned iPads and similar devices agree to abide by the information security guidelines established by the University and supported by UDit.

   a. Users will be required to enable device-level security as outlined by UDit.

   b. Users agree to work cooperatively with UDit to implement and sustain the security procedures as established and supported by UDit, including adherence to the *University of Dayton Policy on Electronic Use of Confidential Data*.

## 4. Device Information Security Overview and Recommendations

UDit continues to identify and evaluate the security practices for mobile devices and will provide updated recommendations on the best practices as better methods emerge and become available.

Mobile device security has three components:

***a) User and Device Security***. Similar to the desktops and laptops we use to do our work each day, we need to make sure mobile devices support the tools our users need to securely access and consume data, as well as provide best practice guidance with respect to how individual devices should be configured. We need to consider security measures such as antivirus, VPN, firewalls, tweak/disable Bluetooth, etc. With mobile devices, we also need to consider whether we want users to be able to install apps and, if so, from where. It's not safe to assume these devices/apps will be malware free.

***b) Enterprise Integration****.* UDit has the responsibility, within the University, to implement and sustain the appropriate infrastructure to secure, control and monitor these devices centrally. Examples include:

   a. Require Authentication/Password Strength
   b. Encryption
   c. Remote Wipe (in the event a device is lost or stolen)
   d. Update Software
   e. Knowledge and tools facilitating support
   f. Screen Lock/timeout
   g. Logging and Auditing

This is done to varying extent for iPhones and Blackberry's with separate infrastructure solutions at present. Google, through their Google Apps suite, provides a relatively unsophisticated, but comprehensive solution for iPhones, Android devices and Windows mobile devices that might allow us to tie all this together.

c) ***The Cloud***[2]. As mobile devices proliferate and become cloud devices, the University has to make sure infrastructure evolves to support those devices with respect to authentication and storage access. This is especially critical for individuals who wish to use mobile devices to access data that contains Personally Identifying, which is subject to control rules (e.g., FERPA, HIPAA, PCI, etc.) or business-sensitive (e.g., research, donor information, salary information, etc.) information. Accessing public data (e.g., published research, electronic journals, general web browsing, etc.) is of less concern.

The iPad is a perfect example. While you can put the Novell client on a laptop, there's no such option for the iPad; thus, it becomes difficult for users to access our current secure enterprise solutions (i.e., Novell home and shared drives) for storing and sharing data. Easy and free solutions (e.g., Google Docs and Dropbox) are available and so users of these devices use and recommend these solutions to others. While these "free" solutions may be technically secure, the university loses control because the data, which may be confidential or business sensitive, is no longer hosted on our servers and subject to our access restrictions and monitoring requirements. Users agree to follow University guidelines on best security practices for cloud-based services.

## 5. Summary

The adoption of these devices may enable many processes and activities associated with our work. However, because these devices introduce new vulnerabilities to our environment, we need to insure that adoption is responsible, informed, and minimizes the likelihood of risk or loss (financial and/or reputation). Users of University-sponsored mobile devices need to work cooperatively with the University information security staff in UDit to ensure that they are applying the best current practices for securing sensitive information. UDit will regularly communicate best security practices to the user community.

[2] "The Cloud" refers to an application or software service that is "hosted" by an internet services company where the application may originate from many different web-based sources. The service could be hosted on many different server distributed in data centers around the world.

## Appendix A: Current state of iPad use in Higher Education

iPads have not achieved widespread adoption in higher education as of January 2011. However, many institutions have initiated various types of “iPad Pilots” that range from small evaluations involving one or two classes to extensive campus-wide long-range studies. The primary focus of these studies are around assessing the devices as course eReaders, as communication and data collection tools and as information access and input devices. Long Island University is one of very few institutions that have deployed these devices campus wide. As of Fall 2010, they distributed 6000 units to all faculty and students. See attached document entitled “iPad Initiatives – Higher Education” for more details.

a) What is the educational and business value of the iPad and Tablet devices?

As with most new technologies, the value in these devices can be assessed in two ways: 1) the added capabilities found in the applications that are available in terms of productivity, efficiencies, cost savings, and enhanced services to customers and 2) the perceived benefit by potential customers in terms of their judgment of the innovativeness and currency of the educational institution and its curricula (Are we using the most current tools & applications?).

A September 2010 Gartner Research Report[3] concludes the following:

> *The Apple iPad and associated ecosystem are likely to disrupt existing technology usage profiles and business models*. *Apple’s iPad is more than just the latest consumer gadget; it is truly disruptive*[4] *and should be seriously examined by every enterprise*. (pg. 1)

***Key Gartner Findings:***

- The Apple iPad is a disruptive device with great appeal and broad functionality. It is not a notebook replacement for the majority of users, but a valuable companion device.
- Individuals are willing to buy these devices themselves, so enterprises must be ready to support them. Recognize the soft benefits of a device of this type in the quest to improve recruitment and retention. Technology is not always about productivity.
- The device is much less intrusive in face-to-face environments than conventional notebooks, making it well suited to a sales or information-sharing environment.

***Gartner Recommendations:***

- Purchase iPads for yourself and a few close associates, and become familiar with this device and what it can (and cannot) do.

[3] Prentice, Stephen (24 September 2011) “CEO Advisory: Seize the iPad Opportunity Now.” Gartner Research ID G00206555.

[4] The term “disruptive” is used to indicate the potential impact of the new technology on displacing older technologies and establishing new patterns of behavior among adopters.

- Request that your marketing and product development teams present a creative briefing within two months detailing how iPads could be used by your company and competitors in your industry.
- Unless there is a self-evident case to the contrary, require your CIO to provide (at a minimum) “concierge” – level iPad support for a limited number of key users, and prepare a budgeted plan for widespread support by mid-2011.

Act sooner rather than later. The cost of early action is low, while the price of delay may well be extremely high.

References:

- http://images.apple.com/ipad/business/pdf/iPad_Security_Overview.pdf
- https://wiki.internet2.edu/confluence/display/itsg2/Mobile+Device+Security
- http://www.baselinemag.com/c/a/Mobile-and-Wireless/10-Best-Practices-for-Mobile-Device-Security/2/
- http://csrc.nist.gov/news_events/HIPAA-May2009_workshop/presentations/7-051909-new-technologies-mobile-devices.pdf
- http://www.sophos.com/security/topic/iphone-blackberry.html
- http://www.alienvault.com/blog/jaime/Malware/Inside_Geinimi_Android_Trojan_Chapter_Two_How_to_check_remotely_the_presence_of_the_trojan.html