

PALM BEACH STATE COLLEGE

ADMINISTRATIVE PROCEDURE

Policy: 6Hx-18-1.XX	Category: Information Technology	Version Date: 0001
Title: Wireless		Effective Date: 11-01-09
Originating Unit: Information Technology Security Office		Last Review: TBD
Review Officer: Chief Information Officer, Anthony Parziale		Next Review: TBD

Overview:

This policy applies to all employees involved in the establishment, maintenance and use of wireless networking technology.

Purpose:

The purpose of this document is to establish administrative procedures for the secure implementation and use of wireless technologies for the Palm Beach State College computing environment.

Guidelines:

Access to Wireless Networks

Approved Wireless Devices

Only those devices (notebooks, handhelds, portables, personal digital assistants, smart phones, etc.) that have been approved for use by the Information Technology Department will be permitted to gain access to the Palm Beach State internal network via wireless technology. These devices must have been pre-configured with the necessary operating system and security software. This software includes, but is not limited to, software that provides an encrypted tunnel (virtual private network) for network traffic, that encrypts device hard drives, that screens for and eradicates computer viruses and other malware, that supports extended user authentication dialogs, that supports remote file backups, that updates software when the software resident on the device is out-of-date, that prevents the user from reconfiguring a device's software, and that logs security-relevant events.

Approved Technical Configuration of Wireless Devices

Only those users who have requested and received Information Technology Department approval for wireless network access will be granted such access. These users must then employ the properly configured machines mentioned above, machines whose internal hardware address (MAC address) is recognized by the wireless network, if they are to

successfully gain wireless network access. Users are prohibited from setting up their own wireless networks without this approval process, whether or not these networks connect with the Palm Beach State internal network.

Access to Palm Beach State internal networks via a wireless connection will furthermore only be permitted in those instances in which the end user employs extended user authentication technology (dynamic password tokens, biometrics, etc.) approved by the Information Technology Security Office (ITSO). This technology goes beyond traditional fixed passwords, and helps to ensure that only authorized people gain access to Palm Beach State computers and networks. Users who have lost a connection to an internal wireless network for five minutes, perhaps because they moved beyond the wireless network coverage area, will in all instances be required to authenticate themselves with this same technology when they reestablish a connection.

Training Required for Wireless Access

In addition, all users granted wireless access to Palm Beach State's internal network must complete a brief wireless network training and awareness program developed by and delivered by the ITSO. After they have completed this program, users will be required to sign a usage agreement promising that they will abide by Palm Beach State information security and privacy requirements. After this signed usage agreement has been received, and the involved users have successfully passed the tests included as part of the training and awareness program, then their wireless network usage will be enabled.

Guest Wireless Privileges

As the above policy statements imply, guest access to Palm Beach State wireless networks is not supported or allowed. An exception is made in certain public areas, such as the headquarters building reception and meeting room area. For the establishment of all of these exception areas, previous approval must be obtained from IT. Wireless networks in these exception areas must provide only public Internet access, not any direct access to internal Palm Beach State computers or networks.

Secure Default Configuration of Wireless Devices

Systems that automatically exchange data between devices via wireless connections -- such as a data synchronization process (also known as a docking process) between a personal digital assistant and a desktop personal computer -- must not be enabled unless these systems have been evaluated and approved by the ITSO. Users should be aware that the use of this and all other types of wireless technology, if it has not been approved as mentioned above, could subject the transmitted data to interception by unauthorized parties, as well as generate signals that could interfere with authorized wireless

networks in the immediate vicinity. For these same reasons, the wireless communications capabilities found in desktop machines and all other Palm Beach State computers must remain disabled until they have been evaluated and approved by the ITSO.

Loss and Recovery of Wireless Technology

Whenever a wireless-enabled computing device (notebook, portable, personal digital assistant, smart phone, etc.) that has been granted access to the Palm Beach State internal network is lost or stolen, this fact must immediately be reported to the Physical Security Department. Users must diligently protect these mobile devices from loss, theft, and tampering. This effort includes not leaving unattended devices in the open in public areas such as airports or trains, and not leaving these devices in hotel rooms when the rooms are unattended. These devices should be deposited in hotel room safes when not in use, locked in file cabinets when not being used in the office, and locked-up in the trunk of a car whenever the car is parked.

Establishing Wireless Networks

Requesting Approval For A Wireless Network

If a wireless network appears to be a good solution to a business problem, a request for a feasibility study examining the use of a wireless network must first be submitted to the Information Technology Department. If this study indicates that a wireless network is a prudent technology that will serve Palm Beach State business needs, a risk assessment must then be performed by the ITSO prior to the deployment of any wireless networks.

Employees who are considering the use of wireless networks for production applications, should be aware that the cost of these systems exceeds that of the wireless network alone. All wireless networks used for production applications must also employ an alternative fail-over networking technology. This will allow business activities to continue when the wireless network is inoperable (for instance due to radio frequency interference). Such a fail-over network must be built, thoroughly tested, and then approved by the ITSO before a wireless network will be permitted to operate with a production application.

Automatic Discovery of Wireless Networks

To enforce this policy, Palm Beach State automatically detects the presence of all internal-network-connected devices, and it refuses network communication services to those devices that have not been formally approved by both the Information Technology Department and the ITSO. To further ensure that all internal wireless networks have

been registered and approved, Palm Beach State periodically conducts "war driving" tests to discover unauthorized wireless access points.

Procurement of wireless technology

Users must not purchase, rent, or otherwise procure wireless equipment on their own. These procurements of hardware, software, and services related to wireless networks must be channeled through the Purchasing Department. This process helps to ensure that these purchases are consistent with existing internal technical standards and security requirements.

Wireless Networks Must Not Process Sensitive Data

Employees who are considering making a request for a wireless network should be aware that wireless networks are not appropriate for Palm Beach State applications that process sensitive data (credit card numbers, bank account numbers, mergers and acquisitions plans, etc.). Reflecting the fact that the security of wireless networks is not as strong as the security of wired networks, the Information Technology Department will deny all requests for wireless networks that are intended to transmit or receive sensitive information.

Installing & Configuring A Wireless Network

Approved personnel only

All wireless access points must be installed by and configured by an authorized member of Palm Beach State systems administration staff or authorized contractors. These people must follow the ITSO's installation, configuration, and management guide for wireless networks. This guide covers a wide variety of topics such as changing default passwords so that unauthorized parties cannot gain system access, turning on encryption so that transmissions are always obscured from wiretappers, and disabling identifier broadcasting so that unauthorized parties cannot readily detect the presence of a wireless network.

Logical and Physical Security of Wireless Access Points

To prevent tampering, reconfiguration, theft, and other unauthorized activity, all wireless network access points must be physically secured in areas accessible only by authorized personnel. Wireless network access points must also be placed, and the wireless coverage area designed, so that the possibility of unauthorized signal interception is minimized.

All wireless access points must be logically distinguished from, and walled off from, the main internal Palm Beach State internal network using configurations approved by the ITSO. Palm Beach State wireless network access points must always be configured so that they consistently employ communications encryption, firewalls, hardware device address (MAC address) filtering, intrusion detection systems, and other security measures defined by the ITSO.

Software Requirements for Wireless Access Points

All wireless access points must be running the latest version of the vendor-supplied operating system and security software. Likewise, all mobile devices authorized to access Palm Beach State wireless networks must be running an up-to-date suite of operating system and security software defined by the ITSO. Those wireless access points or mobile devices that are not running up-to-date software will be blocked from accessing the Palm Beach State internal network. Automatic download facilities must be provided to enable these machines to quickly and securely update their software. In the event that the security of any wireless device has been compromised, these devices will be isolated from the internal network using the same blocking technology, so that further problems are prevented.

Security measures on Palm Beach State production wireless connected systems must not be backward compatible. By forbidding the backwards compatibility of software, Palm Beach State helps to ensure that only the latest versions of operating system and security software is employed. Backwards compatibility means that older software can still be used, and this also means that certain security measures are turned off, unavailable, or inactivated.

Testing of Wireless Networks

Prior to cut-over to production usage of a wireless network, an extensive test must be performed to ensure that all security and availability control mechanisms are working as they are intended to work. Only after the ITSO approves the successful completion of these tests can a wireless network be used for production information processing activities.

Managing A Wireless Network

Authorized Personnel

The management, repair and administration of Palm Beach State wireless networks must be performed by authorized Palm Beach State systems administration staff or authorized contractors. These efforts must follow the procedures defined in the ITSO's installation,

configuration, and management guide for wireless networks. To ensure that wireless networks have been properly configured and managed, periodic audits will be conducted by the Internal Audit Department.

Change Control

Changes to the configuration or set-up of a wireless network must follow the standard change control process that is required for other production information systems. Those authorized systems administrators or authorized contractors who make changes without going through the change control process will find that the involved machines will be blocked from accessing Palm Beach State's internal network. This blocking will be provided with the aid of both network-based auto-discovery software and security auditing software.

All wireless access points must have sufficient disk space and internal resources to support the logging and systems monitoring software specified by the ITSO. Intrusion detection and incident response activities must be managed by and coordinated with the ITSO. Systems administrators responsible for wireless access points must follow the lead of the ITSO in response to all security relevant events such as a denial of service attack, a computer virus infestation, or an intrusion by an unauthorized party.

Inventory of Wireless Equipment

The Information Technology Department must keep an up-to-date inventory of all internal-network-connected equipment including authorized wireless access points and authorized mobile devices that have wireless computing interfaces. This inventory must also indicate the software resident on these devices. Auto-discovery systems must be employed to download the most up-to-date software to these same systems.

Loss and Recovery of Wireless Technology

Mobile devices with wireless communications interfaces that have been reported as lost or stolen must be automatically barred from accessing the Palm Beach State internal network. Poison pill technology must also be employed such that the data resident on these machines will be automatically erased whenever the devices have been reported as lost or stolen.

All wireless access points and mobile devices must also be etched with identifiers that will allow them to be readily returned to Palm Beach State if they are recovered by police or other third parties following an incident where the devices were lost or stolen.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Contact Information:

Questions, concerns or comments concerning this guideline should be directed to:

Tony Parziale

CIO

Palm Beach State College

4200 Congress Avenue, ITB 103

Lake Worth, Florida 33461

Tel: 561.868.3262

Fax: 561.868.3259

Revision History:

Version	Revision Date	Review Date	Description
1.0	06/30/2009		