

# PALM BEACH STATE COLLEGE

## ADMINISTRATIVE PROCEDURE

Policy: 6Hx-18-1.XX	Category: Information Technology	Version Date: 0001
Title: Acceptable Use of Internet Resources		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:

**Opportunities and Risks** – The wide array of new resources, services, and inter-connectivity available through the Internet all introduce new educational and business opportunities, as well as new security and privacy risks. In response to the risks, this administrative procedure describes Palm Beach State College’s official stance regarding Internet security and acceptable use of Internet resources.

**Applicability** – This administrative procedure applies to all employees, contractors, consultants, temporaries, and volunteers, who use the Internet with Palm Beach State computing or networking resources. Within this document, the term “Internet” is used to reference all electronic communications which access the Internet, including web sites, Internet Relay Chat (IRC), message boards, or blogs. This administrative procedure applies to all those who use the Internet and represent themselves as being connected in some way with Palm Beach State. All of these Internet users are expected to be familiar with and fully comply with this administrative procedure. Questions about this administrative procedure should be directed to the College’s Information Security Manager.

**Prior Management Approval** – Palm Beach State users must not access the Internet without a proper understanding of the associated personal and business risks. In order to receive Internet access privileges, all employees must complete the Palm Beach State new-hire orientation course. Access to the Internet, aside from electronic mail, will be provided to only those employees who have a legitimate business need for such access. The ability to access the Internet and engage in other Internet activities is not a fringe benefit to which all employees are entitled. If an employee does not have sufficient Internet access, but needs access for a particular project, he or she can request temporary elevated access, subject to management’s approval.

### Purpose:

The purpose of this administrative procedure is to establish a standard for acceptable use of Internet resources by Palm Beach State personnel.

### Scope:

This administrative procedure is applicable to all Palm Beach State faculty and staff users, and encompasses use of Internet access through college resources.

## **Guidelines:**

### ***Information Integrity***

**Information Reliability** – All information acquired from the Internet must be considered suspect until confirmed by separate information from another source. Before using free Internet-supplied information for College business decision-making purposes, employees should corroborate the information by consulting other sources.

**Virus Checking** – All non-text files downloaded from non-Palm Beach State sources through the Internet must be screened with current virus detection software prior to being used. Whenever an external provider of the software is not trusted, downloaded software must be tested on a stand-alone, non-production machine that has been recently backed up. Downloaded files must be decrypted and decompressed before being screened for viruses. The use of digital signatures to verify that a file has not been altered by unauthorized parties is recommended, but this does not assure freedom from viruses, Trojan horses, and other problems.

**Software Downloading** – Palm Beach State has implemented an automatic software distribution system to install the latest release of licensed software on Palm Beach State computers. A separate system is used to automatically trace all software resident on these same systems. As discussed in the Information Security Policy, employees must not install software on their Palm Beach State-supplied computers, whether the software was downloaded from the Internet or procured elsewhere.

**Push Technology** – Automatic updating of software or information on Palm Beach State computers through background push Internet technology is prohibited unless the involved system has been tested and approved for distribution by the Information Technology department.

**Spoofing Users** – Before employees release any internal Palm Beach State information, enter into any contracts, or order any products through public networks, the identity of the individuals and organizations contacted must be confirmed. Identity confirmation is ideally performed through digital signatures or digital certificates, but in cases where these are not available, other means such as letters of credit, third-party references, and telephone conversations may be used.

**User Anonymity** – Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any Palm Beach State electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings. If users have a need to employ remailers or other anonymous facilities, they must do so on their own time, with their own information systems and

## Palm Beach State **Acceptable Use of Internet Resource**

Internet service provider accounts. Use of anonymous FTP logons, anonymous UUCP logons, HTTP or web browsing, and other access methods established with the expectation that users would be anonymous are not permissible.

**Electronic Mail Attachments** – Employees must not open electronic mail attachments unless they were expected from a trusted sender. When they are expected from a known and trusted sender, attachments must be scanned with a virus package prior to being opened.

**Responding to Information Requests** – Employees must never respond to unsolicited requests for personal information, including passwords or credit card numbers, from an electronic mail message. Any such message should be immediately reported to the Information Technology Security Office.

**Web Page Changes** – Employees must not establish new Internet pages dealing with Palm Beach State business, or make modifications to existing web pages dealing with Palm Beach State business, unless they have obtained the approval of the Information Technology and College Relations and Marketing departments. Modifications include the addition of links to other sites, updating the information displayed, and altering the graphic layout of a page. This committee must ensure that all posted material has a consistent and polished appearance, is aligned with business goals, and is protected with adequate security measures.

**Web Page Archives** – Every version of the Palm Beach State Internet site and commerce site files must be securely archived in two physically separated locations. Information Technology will designate a web master who will keep this archive and provide copies of historical pages on demand.

### **Information Confidentiality**

**Information Exchange** – Palm Beach State software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-Palm Beach State party for any purposes other than business purposes expressly authorized by management. Exchanges of software or data between Palm Beach State and any third party must not proceed unless a written agreement has been signed. Such an agreement must specify the terms of the exchange, and the ways that the software or data is to be handled and protected. Regular business practices, need not involve such a specific agreement since the terms and conditions are implied.

**Posting Materials** – Employees must not post unencrypted Palm Beach State material on any publicly-accessible Internet computer that supports anonymous FTP or similar publicly-accessible services, unless the posting of these materials has been approved by the director of Public Relations. Palm Beach State internal information must not be placed in any computer unless the persons who have access to that computer have a legitimate business need to know the involved information.

**Message Interception** – Palm Beach State secret, proprietary, or private information must not be sent over the Internet unless it has been encrypted by approved methods. Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet. For the same reasons, Internet telephone services must not be used for Palm Beach State business unless the connection is known to be encrypted.

**Security Parameters** – Unless a connection is known to be encrypted, security parameters and other sensitive data that can be used to gain access to goods or services, must not be sent over the Internet in readable form. Encryption processes are permissible if they are approved by the College Information Security Manager.

## **Public Representations**

**External Representations** – Employees may indicate their affiliation with Palm Beach State in mailing lists, chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for example through an electronic mail address. In either case, whenever employees provide an affiliation, unless they have been expressly designated as a spokes-person of Palm Beach State, they also must clearly indicate the opinions expressed are their own, and not necessarily those of Palm Beach State. If an affiliation with Palm Beach State is provided, political advocacy statements and product or service endorsements also are prohibited unless they have been previously cleared by the director of College Relations and Marketing. With the exception of ordinary marketing and customer service activities, all representations on behalf of Palm Beach State must be cleared by the director of Public Relations.

**Private Email Addresses** – Employees posting information on any publicly available web site must not include their personal Palm Beach State electronic mail address. These postings are used to generate SPAM against Palm Beach State. Palm Beach State issues separate email addresses for specific public postings. Users who require the external posting of their personal email address must request permission from their manager or College Relations and Marketing.

**Appropriate Behavior** – Whenever any affiliation with Palm Beach State is included with an Internet message or posting, written attacks are strictly prohibited. Employees must not make threats against another user or organization over the Internet. All Internet messages intended to harass, annoy, or alarm another person are similarly prohibited.

**Removal Of Postings** – Those messages sent to Internet discussion groups, electronic bulletin boards, or other public forums, that include an implied or explicit affiliation with Palm Beach State, may be removed if management deems them to be inconsistent with Palm Beach State business interests or existing College policies and procedures. Messages in this category include political statements, religious statements, cursing or other foul language, and statements viewed as harassing others based on race, creed,

color, age, sex, physical handicap, or sexual orientation. The decision to remove electronic mail must be made by the College Information Security Manager or the director of Human Resources. When practical and feasible, individuals responsible for the message will be informed of the decision and given the opportunity to remove the message themselves.

**Disclosing Internal Information** – Employees must not publicly disclose internal Palm Beach State information through the Internet that may adversely affect Palm Beach State customer relations or public image unless the approval of the director of College Relations and Marketing or a member of the Executive Leadership Council has been obtained. Such information includes College business activities, research and development, internal performance analyses, and internal information systems problems. Responses to specific customer electronic mail messages are exempted from this administrative procedure.

**Inadvertent Disclosure** – Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, Usenet, and related public postings on the Internet. Before posting any material, employees must consider whether the posting could cause Palm Beach State embarrassment and/or public relations problems. Employees should keep in mind that several separate pieces of information can be pieced together to form a picture revealing confidential information that then could be used against Palm Beach State. Employees must never post on the Internet the specific computer or network products employed by Palm Beach State.

## **Intellectual Property Rights**

**Copyrights** – When at work, or when Palm Beach State computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. Off-hours participation in pirate software bulletin boards and similar activities represent a conflict of interest with Palm Beach State work, and are therefore prohibited. The reproduction, forwarding, or in any other way republishing or redistribution of words, graphics, or other copyrighted materials must be done only with the permission of the author or Owner. Employees must assume that all materials on the Internet are copyrighted unless specific notice states otherwise. When information from the Internet is integrated into internal reports or used for other purposes, all material must include labels such as "copyright, all rights reserved" and specifics about the source of the information.

**Publicly-Writable Directories** – All publicly-writable directories on Palm Beach State Internet-connected computers must be reviewed and cleared each evening. Employees using Palm Beach State computers must not be involved in any way with the exchange of pirated software, multi-media, purloined passwords, stolen credit card numbers, and inappropriate written or graphic material.

## **Access Control**

**Inbound User Authentication** – All users wishing to establish a real-time connection with Palm Beach State internal computers through the Internet must employ a virtual private network (VPN) product approved by the ITSO that can encrypt all traffic exchanged. These VPN products also must authenticate remote users at a firewall before permitting access to the Palm Beach State internal network. This authentication process must be achieved through a dynamic password system approved by the College Information Security Manager. Examples of approved technology include hand-held smart cards with dynamic passwords and user-transparent challenge and response systems. Designated public systems do not need user authentication processes because anonymous interactions are expected.

**Remote Machine Security** – Employees who have not installed required software patches or upgrades, or whose systems are virus-infested, must be disconnected automatically from the Palm Beach State network until they have reestablished a secure computing environment. The computers used by all employees employing VPN technology must be remotely scanned automatically to determine that the software is current and that the system has been properly secured.

**Restriction Of Third-Party Access** – Inbound Internet access privileges must not be granted to third-party vendors, contractors, consultants, temporaries, outsourcing organization personnel or other third parties unless the relevant system manager determines that these individuals have a legitimate business need for such access. These privileges must be enabled only for specific individuals and only for the time period required to accomplish approved tasks.

**Browser User Authentication** – Employees must not save fixed passwords in their web browsers or electronic mail clients. These fixed passwords must be provided each time that a browser or electronic mail client is invoked. Browser passwords may be saved if a boot password must be provided each time the computer is powered up, and if a screen saver password must be provided each time the system is inactive for a specified period of time. Palm Beach State computer users must refuse all offers by software to place a cookie on their computer so that they can automatically log on the next time that they visit a particular Internet site. Cookies that serve other purposes are permissible.

**Data Aggregators** – Users must not provide their Internet user IDs and passwords to data aggregators, data summarization and formatting services, or any other third parties.

**Internet Service Providers** – With the exception of telecommuters and mobile computer users, employees must not employ Internet service provider accounts, dial-up lines, and wireless devices to access the Internet with Palm Beach State computers. All Internet activity must pass through Palm Beach State firewalls so that access controls and related security mechanisms can be applied. Users must employ their Palm Beach State

Palm Beach State **Acceptable Use of Internet Resource**

electronic mail address College related business. Use of a personal electronic mail address for this purpose is prohibited.

**Establishing Network Connections** – Unless the prior approval of the Information Technology department has been obtained, employees must not establish Internet or other external network connections that could permit non-Palm Beach State users to gain access to Palm Beach State systems and information. These connections include the establishment of multi-computer file systems, Internet pages, Internet commerce systems, FTP servers, and wireless access points.

**Conducting Business Over The Internet** – Unless advance approval of the Purchasing department has been obtained, Palm Beach State employees must not purchase any goods or services through the Internet if these goods or services are offered by a business based in, or operating out of, a foreign country.

## **Personal Use**

**Personal Use** – Employees who have been granted Internet access and who wish to explore the Internet for personal purposes must do so on personal rather than company time. Games, news groups, and other non-business activities must be performed on personal, not company time. Use of Palm Beach State computing resources for these personal purposes is permissible as long as the incremental cost of the usage is negligible, no Palm Beach State business activity is preempted by the personal use, and the usage is not likely to cause either a hostile working environment or a poor behavioral example. Employees must not employ the Internet or other internal information systems in such a way that the productivity of other employees is eroded. Examples of this include chain letters and broadcast charitable solicitations. Palm Beach State computing resources must not be resold to other parties or used for any personal business purposes such as running a consulting business on off-hours.

**Offensive Web Sites** – Palm Beach State is not responsible for the content that employees may encounter when they use the Internet. When and if users make a connection with web sites containing objectionable content, they must promptly move to another site or terminate their session. Employees using Palm Beach State computers who discover they have connected with a web site that contains sexually explicit, racist, sexist, violent, or other potentially offensive material must immediately disconnect from that site.

**Blocking Sites and Content Types** – The ability to connect with a specific web site does not in itself imply that users of Palm Beach State systems are permitted to visit that site. Palm Beach State may, at its discretion, restrict or block the downloading of certain sites and/or file types that are likely to cause network service degradation. These file types may include graphic and music files.

**Use of “social networking” sites** – Users are prohibited from accessing web sites designed for the sole purpose of posting and sharing personal information. Exceptions

require the approval of the ITSO and must be for documented business purposes. Palm Beach State reserves the right to block access to these or other web sites. Employees are also prohibited from discussing specific Palm Beach State business within any personal home pages they may have established on these sites outside of Palm Beach State business hours.

## **Privacy Expectations**

**No Default Protection** – Employees using Palm Beach State information systems or the Internet must realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, employees must not send information over the Internet if they consider it to be confidential or private.

**Management Review** – At any time and without prior notice, Palm Beach State management reserves the right to examine electronic mail messages, files on personal computers, web browser cache files, web browser bookmarks, logs of web sites visited, computer system configurations, and other information stored on or passing through Palm Beach State computers.

**Logging** – Palm Beach State routinely logs the web sites visited, files downloaded, time spent on the Internet, and related information. Department managers may receive reports of such information and use it to determine what types of Internet usage are appropriate for their department's business activities.

**Junk Electronic Mail** – Users must not use Palm Beach State computer systems for the transmission of unsolicited bulk electronic mail advertisements or commercial messages that are likely to trigger complaints from the recipients. These prohibited messages include a wide variety of unsolicited promotions and solicitations such as chain letters, pyramid schemes, and direct marketing pitches. When employees receive unwanted and unsolicited electronic mail, they must refrain from responding directly to the sender. They must forward the message to the iTAC at Palm Beach State who then can take steps to prevent further transmissions.

## **Reporting Security Problems**

**Notification Process** – If sensitive Palm Beach State information is lost, disclosed to unauthorized parties, or suspected of either, the Information Security Manager must be notified immediately. If any unauthorized use of Palm Beach State information systems has or is suspected of taking place, the College Information Security Manager must be notified immediately. Whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the College Information Security Manager must be notified immediately. All unusual systems behavior, such as missing files, frequent system crashes, and misrouted

Palm Beach State **Acceptable Use of Internet Resource**

messages must be immediately reported to the iTAC. The specifics of security problems must not be discussed widely but should instead be shared on a need-to-know basis.

**False Security Reports** – Employees in receipt of information about system vulnerabilities must forward it to the College Information Security Manager, who then will determine what if any action is appropriate. Employees must not personally redistribute system vulnerability information to other users.

**Testing Controls** – Employees must not test or probe security mechanisms at either Palm Beach State or other Internet sites unless they have obtained written permission from the College Information Security Manager. The possession or the usage of tools for detecting information system vulnerabilities, or tools for compromising information security mechanisms, are prohibited without the advance permission of the College Information Security Manager.

### **Enforcement**

Violations of this administrative procedure can lead to revocation of system privileges or additional disciplinary action up to and including termination.

### **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: 561.868.3239

Fax: 561.868.3259

### **Revision History:**

<b>Version</b>	<b>Revision Date</b>	<b>Review Date</b>	<b>Description</b>
1.0	06/30/2009		