

PALM BEACH STATE COLLEGE

ADMINISTRATIVE PROCEDURE

Procedure: 6Hx-18-1.XX	Category: Information Technology	Version Date: 0001
Title: Information Security Administrative Procedure		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:

Role Of Information And Information Systems - Palm Beach State College is critically dependent on information and information systems. If important information were disclosed to inappropriate persons, the College could suffer considerable damage and/or serious losses. The excellent reputation that Palm Beach State enjoys is also directly linked with the way that it manages both information and information systems. For example, if student information were to be publicly disclosed, the organization's reputation would be harmed. For these and other important operational reasons, College executive management working in conjunction with the board of trustees has initiated and continues to support an information security effort. One part of that effort is the definition of the College's information security policies and procedures.

Team Effort - To be effective, information security must be a team effort involving the participation and support of every Palm Beach State employee who deals with information and information systems. In recognition of the need for teamwork, this administrative procedure statement clarifies the responsibilities of users and the steps they must take to help protect Palm Beach State information and information systems. This document describes ways to prevent and respond to a variety of threats to information and information systems including unauthorized access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and denial of use.

Scope:

Involved Persons – Palm Beach State employees must comply with the information security procedures found in this and related information security documents.

Involved Systems - This procedure applies to all computer and network systems owned by or administered by Palm Beach State. This procedure applies to all operating and application systems. The procedure covers only information handled by computers and networks. Although this document includes mention of other manifestations of information such as voice and paper, it does not directly address the security of information in these forms. For information about the protection of information in paper form, see the Data Classification Procedures.

Responsibilities

Primary Departments Working On Information Security - Guidance, direction, and authority for information security activities are centralized for all Palm Beach State organizational units in the Information Technology Security Office (ITSO). ITSO is responsible for establishing and maintaining organization-wide information security policies, standards, guidelines, and procedures. Investigations of system intrusions and other information security incidents are the responsibility of the ITSO, with support from other IT groups, as identified in the organization's Information Security Incident Response procedures

Three Categories Of Responsibilities - To coordinate a team effort, Palm Beach State has established three categories, at least one of which applies to each employee. These categories are Owner, Custodian, and User. These categories define general responsibilities with respect to information security.

Owner Responsibilities - Information Owners are the department managers, members of the top management team, or their delegates within Palm Beach State who bear responsibility for the acquisition, development, and maintenance of production applications that process Palm Beach State information. Production applications are computer programs that regularly provide reports in support of decision making and other business activities. All production application system information must have a designated Owner. For each type of information, Owners designate the relevant sensitivity classification, designate the appropriate level of criticality, define which users will be granted access, and approve requests for various ways in which the information will be utilized.

Custodian Responsibilities - Custodians are in physical or logical possession of either Palm Beach State information or information that has been entrusted to Palm Beach State. While Information Technology department staff members clearly are Custodians, local system administrators are also Custodians. Whenever information is maintained only on a personal computer, the User is also a Custodian. Each type of production application system information must have one or more designated Custodians. Custodians are responsible for safeguarding the information, including implementing and maintaining access control systems to prevent inappropriate disclosure, and making backups so that critical information will not be lost. Custodians are also required to implement, operate, and maintain appropriate security measures.

User Responsibilities - Users are responsible for familiarizing themselves with and complying with all Palm Beach State policies, procedures, and standards dealing with information security. Questions about the appropriate handling of a specific type of

information should be directed to either the Custodian or the Owner of the involved information.

Information Classification and Handling

Consistent Information Handling - Palm Beach State information, and information that has been entrusted to Palm Beach State, must be protected in a manner commensurate with its sensitivity and criticality. Security measures must be employed regardless of the media on which information is stored, the systems that process it, or the methods by which it is moved. Information must be protected in a manner that is consistent with its classification, no matter what its stage in the life cycle from origination to destruction.

Information Classification Designations - Palm Beach State has adopted an information classification system that categorizes information into four groupings. All information under Palm Beach State control, whether generated internally or externally, falls into one of these categories: Secret, Confidential, Internal Use Only, or Public. All employees must familiarize themselves with the definitions for these categories and the steps that must be taken to protect the information falling into each of these categories. Details can be found in the Data Classification Procedures . For purposes of this procedure, “sensitive information” is information that falls into either the Secret or Confidential categories.

Information Classification Labeling - If information is sensitive, from the time it is created until the time it is destroyed or declassified, it must be labeled with an appropriate information classification designation. Such markings must appear on all manifestations of the information. The vast majority of Palm Beach State information falls into the Internal Use Only category. For this reason, it is not necessary to apply a label to Internal Use Only information. Information without a label is therefore by default classified as Internal Use Only. Further instructions about labeling sensitive information can be found in the Data Classification Procedure.

Information Access Control

Need to Know - Access to information in the possession of, or under the control of, Palm Beach State must be provided based on the need to know. Information must be disclosed only to people who have a legitimate business need for the information. At the same time, employees must not withhold access to information when the Owner of the information instructs that it be shared. To implement the need-to-know concept, Palm Beach State will adopt an access request and Owner approval process. Employees must not attempt to access sensitive information unless the relevant Owner has granted them access rights. When an employee changes job duties, including termination, transfer,

promotion and leave of absence, his or her supervisor must immediately notify the HR and IT. The privileges granted to all employees must be periodically reviewed by information Owners and Custodians to ensure that only those with a current need to know presently have access.

User IDs And Passwords - To implement the need-to-know process, Palm Beach State requires that each employee accessing multi-user information systems have a unique user ID and a private password. These user IDs must be employed to restrict system privileges based on job duties, project responsibilities, and other business activities. Each employee is personally responsible for the usage of his or her user ID and password.

Anonymous User IDs - With the exception of electronic bulletin boards, Internet sites, intranet sites, and other systems where all regular users are intended to be anonymous, users are prohibited from logging into any Palm Beach State system or network anonymously. Anonymous access might, for example, involve use of "guest" user IDs. When users employ system commands that permit them to change active user IDs to gain certain privileges, they must have initially logged on employing user IDs that clearly indicated their identities.

Difficult-to-Guess Passwords - Users must choose passwords that are difficult to guess. This means that passwords must not be related to one's job or personal life. For example, a car license plate number, a spouse's name, birth dates, or fragments of an address must not be used. This also means passwords must not be a word found in the dictionary or some other part of speech. For example, proper names, places, technical terms, and slang must not be used.

Easily Remembered Passwords - Users can choose easily-remembered passwords that are at the same time difficult for unauthorized parties to guess if they:

- string several words together into a pass-phrase
- shift the input of a word up, down, left, or right one row on the keyboard
- bump characters in a word a certain number of letters up or down the alphabet
- transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the word
- combine punctuation, symbols and/or numbers with a regular word
- create acronyms from words in a song, poem, or another known sequence of words
- deliberately misspell a word
- combine several preferences like hours of sleep desired and favorite colors.

Repeated Password Patterns - Users must not construct passwords with a basic sequence of characters that is then partially changed based on the date or some other

predictable factor. Users must not construct passwords that are identical or substantially similar to passwords they have previously employed.

Password Constraints - Passwords must be at least 8 characters long. Passwords must be changed every 45 days or at more frequent intervals. Whenever an employee suspects that a password has become known to another person, that password must immediately be changed.

Password Storage - Passwords must not be stored in readable form in batch files, automatic logon scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorized persons might discover them. Passwords must not be written down in some readily-decipherable form and left in a place where unauthorized persons might discover them (e.g. on post-it notes, under the keyboard, etc.)

Sharing Passwords - If employees need to share computer-resident data, they must use electronic mail, collaborative databases, public directories on local area network servers, and other mechanisms approved for such use. System administrators and other technical information systems staff must never ask an employee to reveal their personal password. The only time when a password should be known by another is when it is issued. These temporary passwords must be changed the first time that the authorized user accesses the system. If a user believes that his or her user ID and password are being used by someone else, the user must immediately notify the system administrator for the information system.

Compliance Statement - All employees who wish to use Palm Beach State multi-user computer systems must sign an acceptable use agreement prior to being issued a user ID. Where users already have user IDs, such signatures must be obtained prior to receiving annually-renewed user IDs. A signature on this compliance statement indicates the involved user understands and agrees to adhere to Palm Beach State policies and procedures related to computers and networks, including the instructions contained in this procedure.

Third Party Data Handling

Release Of Information To Third Parties - Unless it has specifically been designated as public, all Palm Beach State internal information must be protected from disclosure to third parties. Third parties may be given access to Palm Beach State internal information only when a demonstrable need to know exists, when a Palm Beach State non-disclosure agreement has been signed, and when such a disclosure has been expressly authorized by the relevant Palm Beach State information Owner. If sensitive information is lost, is disclosed to unauthorized parties, or is suspected of being lost or disclosed to

unauthorized parties, the information Owner and the ITSO must be notified immediately.

Third-Party Requests For Palm Beach State Information - Unless an employee has been authorized by the information Owner to make public disclosures, all requests for information about Palm Beach State and its business must be referred to the College Relations and Marketing department. Such requests include questionnaires, surveys, and newspaper interviews. This procedure does not apply to sales and marketing information about Palm Beach State products and services, nor does it pertain to technical support calls. If an employee is to receive sensitive information from third parties on behalf of Palm Beach State, this receipt must be preceded by the third-party signature on a Palm Beach State release form.

External Disclosure Of Security Information - Information about security measures for Palm Beach State computer and network systems is confidential and must not be released to people who are not authorized users of the involved systems unless approved by the Information Security Manager. For example, publishing external system access information in directories is prohibited. Public disclosure of electronic mail addresses is permissible for College business purposes.

Physical Security

Physical Security to Control Information Access - Access to every office, data center, and other Palm Beach State work areas containing sensitive information must be physically restricted to those people with a need to know. When not in use, sensitive information must always be protected from unauthorized disclosure. When left in an unattended room, sensitive information in paper form must be locked away in appropriate containers. If a Custodian of such information believes he or she will be away for less than 30 minutes, information in paper form may be left on a desk or in some other readily observed spot only if all doors and windows to the unattended room are closed and locked. During non-working hours, employees in areas containing sensitive information must secure all information. Unless information is in active use by authorized people, desks must be clear and clean during non-working hours to prevent unauthorized access to information. Employees must position their computer screens such that unauthorized people cannot look over their shoulder and see the sensitive information displayed.

Theft Protection - All Palm Beach State computer and network equipment must be physically secured with anti-theft devices if located in an open area. Local area network servers and other multi-user systems must be placed in locked cabinets, locked closets, or locked computer rooms. Portable computers must be secured with locking cables,

placed in locking cabinets, or secured by other locking systems when in an open office environment but not in active use.

Network Security

Internal Network Connections - All Palm Beach State computers that store sensitive information, and that are permanently or intermittently connected to internal computer networks, must have a password-based access control system approved by the Information Technology Security Office. Regardless of the network connections, all stand-alone computers handling sensitive information must also employ an approved password-based access control system. Users working with all other types of computers must employ the screen saver passwords that are provided with operating systems, so that after a period of no activity the screen will go blank until the correct password is again entered. Multi-user systems throughout Palm Beach State must employ automatic log off systems that automatically terminate a user's session after a defined period of inactivity.

External Network Connections - All in-bound session connections to internal Palm Beach State resources from external networks must be protected with an approved security measure (e.g., VPN, multi-factor authentication device, etc.) When using Palm Beach State computers, Palm Beach State employees must not establish connections with external networks including Internet service providers unless these connections have been approved by the ITSO.

Network Changes - With the exception of emergency situations, all changes to Palm Beach State computer networks must be documented in a work order request, and approved in advance by the Information Technology department. All emergency changes to Palm Beach State networks must be made only by persons who are authorized by the Information Technology department. This process prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information, and other problems. This process applies not only to employees but also to vendor personnel.

Internet and Electronic Mail

Internet Access - Employees are provided with Internet access to perform their job duties, but this access may be terminated at any time at the discretion of an employee's supervisor, or IT. Internet access is logged and monitored to ensure that employees are not visiting sites unrelated to their jobs, and also to ensure that they continue to be in compliance with security procedures. Employees must take special care to ensure that they do not represent Palm Beach State on Internet discussion groups and in other

Palm Beach State **Information Security Administrative Procedure**

public forums, unless they have previously received top management authorization to act in this capacity. All information received from the Internet should be considered to be suspect until confirmed by reliable sources. Employees must not place Palm Beach State material on any publicly-accessible computer system such as the Internet unless the posting has been approved by both the information Owner and the director of the Information Technology department. The establishment of Internet pages is separately handled by an approval process involving the College Relations and Marketing department]. Users are prohibited from establishing any electronic commerce arrangements over the Internet unless Information Technology and the ITSO have evaluated and approved of such arrangements. Sensitive information, including passwords and credit card numbers, must not be sent across the Internet unless this information is in encrypted form.

Electronic Mail - Every Palm Beach State employee who uses computers in the course of their regular job duties will be granted an Internet electronic mail address and related privileges. All Palm Beach State business communications sent by electronic mail must be sent and received using this company electronic mail address. A personal Internet service provider electronic mail account or any other electronic mail address must not be used for Palm Beach State business unless an employee obtains management approval. When transmitting messages to groups of people outside Palm Beach State, employees must always use either the blind carbon copy facility or the distribution list facility. Unsolicited electronic mail transmissions to prospects and customers are prohibited. Emotional outbursts sent through electronic mail and overloading the electronic mail account of someone through a deluge of messages are forbidden. All business electronic mail communications must be proofread before they are sent, and professional and businesslike in both tone and appearance. Electronic mail is a public communication method much like a postcard. All Palm Beach State employees must refrain from sending credit card numbers, passwords, or other personally identifiable information (PII) that might be intercepted. All Palm Beach State staff must additionally employ a standard electronic mail signature that includes their full name, job title, business address, and business telephone number.

Computer Virus Scanning - All personal computer users must keep the current versions of approved virus screening software enabled on their computers. Users must not abort automatic software processes that update virus signatures. Virus scanning software must be used to scan all software and data files coming from either third parties or other Palm Beach State groups. This scanning must take place before new data files are opened and before new software is executed. Employees must not bypass or turn off the scanning processes that could prevent the transmission of computer viruses.

Computer Virus Removal - If employees suspect infection by a computer virus, they must immediately stop using the involved computer and call the iTAC. Magnetic storage media used with the infected computer must not be used with any other

computer until the virus has been successfully eradicated. The infected computer must also be immediately isolated from internal networks. Users must not attempt to eradicate viruses themselves. Qualified Palm Beach State staff or consultants must complete this task in a manner that minimizes both data destruction and system downtime.

Software Sources - Palm Beach State computers and networks must not run software that comes from sources other than other Palm Beach State departments, knowledgeable and trusted user groups, well-known systems security authorities, or established computer, network, or commercial software vendors. Software downloaded from electronic bulletin boards, shareware, public domain software, and other software from untrusted sources must not be used unless it has been subjected to a rigorous testing regimen approved by the ITSO.

Written Specifications for Owners - All software developed by in-house staff, intended to process critical or sensitive Palm Beach State information, must have a formal written specification. This specification must include discussion of security risks and controls including access control systems and contingency plans. The specification must be part of an agreement between the information Owner and the system developer. Macros in spreadsheets and word processing documents are not considered software in this paragraph.

Security Sign-Off Required - Before being used for production processing, new or substantially changed application systems must have received written approval from the ITSO for the controls to be employed. This requirement applies to personal computers just as it does to larger systems.

Formal Change Control - All computer and communications systems used for production processing must employ a documented change control process that is used to ensure that only authorized changes are made. This change control procedure must be used for all significant changes to production system software, hardware, communications links, and procedures. This procedure applies to personal computers running production systems and larger multi-user systems. For further information on this topic, see the Software Development and Change Control Procedures.

Systems Development Conventions - All production software development and software maintenance activities performed by in-house staff must adhere to Information Technology department policies, standards, procedures, and other systems development conventions. These conventions include proper testing, training, and documentation. For further information on this topic, see the Software Development And Change Control Procedures.

Adequate Licenses - Palm Beach State management must make appropriate arrangements with software vendors for additional licensed copies, if and when additional copies are needed for College business activities.

Unauthorized Copying - Users must not copy software provided by Palm Beach State to any storage media, transfer such software to another computer, or disclose such software to outside parties without advance permission from their supervisor. Ordinary backup copies are an authorized exception to this procedure, provided they are stored on-site in a secured area.

Backup Responsibility - Personal computer users must regularly back up the information on their personal computers, or ensure that someone else is doing this for them. For servers and communication systems, a system administrator is responsible for making periodic backups. If requested, the Information Technology department must install, or provide technical assistance for the installation of approved backup hardware and software. All backups containing critical or sensitive information must be stored at an approved off-site location with either physical access controls or encryption. A contingency plan must be prepared for all applications that handle critical production information. It is the responsibility of the information Owner to ensure that this plan is adequately developed, regularly updated, and periodically tested.

User Rights and Expectations

Rights To Material Developed - While performing services for Palm Beach State, employees must grant to Palm Beach State exclusive rights to patents, copyrights, inventions, or other intellectual property they originate or develop. All programs and documentation generated by, or provided by employees for the benefit of Palm Beach State are the property of Palm Beach State. Palm Beach State asserts the legal ownership of the contents of all information systems under its control. Palm Beach State reserves the right to access and use this information at its discretion.

Right To Search And Monitor - Palm Beach State management reserves the right to monitor, inspect, or search at any time all Palm Beach State information systems. This examination may take place with or without the consent, presence, or knowledge of the involved employees. The information systems subject to such examination include, but are not limited to, electronic mail system files, personal computer hard drive files, voice mail files, printer spool files, fax machine output, desk drawers, and storage areas. All searches of this nature must be conducted after proper approval has been obtained. Because Palm Beach State computers and networks are provided for business purposes only, employees must have no expectation of privacy associated with the information they store in or send through these information systems. Palm Beach State management

Palm Beach State **Information Security Administrative Procedure**

retains the right to remove from its information systems any material it views as offensive or potentially illegal.

Personal Use - Palm Beach State information systems are intended to be used for business purposes only. Incidental personal use is permissible if the use does not consume more than a trivial amount of resources that could otherwise be used for business purposes, does not interfere with employee productivity, and does not preempt any business activity. Permissible incidental use of an electronic mail system would, for example, involve sending a message to schedule a luncheon. Personal use that does not fall into these three categories requires the advance permission of a department manager. Games that are shipped with computer operating systems can be played during scheduled breaks or lunch as long as this activity does not interfere with either employee productivity or intention. Games that take the form of separate software packages are prohibited. Use of Palm Beach State information systems for chain letters, charitable solicitations, political campaign material, religious work, transmission of objectionable material, or any other non-business use is prohibited.

Unbecoming Conduct - Palm Beach State management reserves the right to revoke the system privileges of any user at any time. Conduct that interferes with the normal and proper operation of Palm Beach State information systems, which adversely affects the ability of others to use these information systems, or is harmful or offensive to others is not permitted.

Security Compromise Tools - Unless specifically authorized by the ITSO, Palm Beach State employees must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of such tools include those that defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files. Without this type of approval, employees are prohibited from using any hardware or software that monitors the traffic on a network or the activity on a computer.

Prohibited Activities - Users must not test, or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the ITSO. Incidents involving unapproved system hacking, password guessing, file decryption, bootleg software copying, or similar unauthorized attempts to compromise security measures may be unlawful, and will be considered serious violations of Palm Beach State internal procedure. Short-cuts bypassing systems security measures, and pranks and practical jokes involving the compromise of systems security measures are absolutely prohibited.

Mandatory Reporting - All suspected procedure violations, system intrusions, virus infestations, and other conditions that might jeopardize Palm Beach State information or

Palm Beach State **Information Security Administrative Procedure**

Palm Beach State information systems must be immediately reported to the ITSO (via voice mail 561-868-3262).

Enforcement:

Any employee found to have violated this procedure 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		Initial Procedure Document