

PALM BEACH STATE COLLEGE

ADMINISTRATIVE PROCEDURE

Policy: 6Hx-18-1.XX	Category: Information Technology	Version Date: 0001
Title: Secure Application Development		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:

Palm Beach State College purchases and develops a variety of application software as part of ongoing business operations. These business applications are critical to our business and often contain sensitive information such as customer records, payment information or propriety information. To reduce the risk of accidental disclosure of sensitive information, and to protect Palm Beach State information assets, all Palm Beach State applications must be developed with the highest levels of data security and privacy.

Purpose:

The purpose of this policy is to communicate our organization's requirements for the secure development, testing and deployment of applications developed in-house or by third parties.

All applications, whether internally developed, vendor-acquired, or contracted for, should be subject to appropriate security risk assessment and mitigation processes. Vulnerabilities in applications increase operational and reputation risk as unplanned or unknown weaknesses may compromise the confidentiality, availability, and integrity of data. Although this guidance is focused on the risks and risk management techniques associated with Web-based applications, the principles are applicable to all types of software.

Scope:

This policy applies to employees, contractors, consultants, temporaries, and other workers at Palm Beach State which are involved in the design, development or testing of business applications. This policy applies to all production business applications purchased, owned or developed by Palm Beach State.

Policy:

Roles and Responsibilities

Employee Responsibilities – All employees who are involved the specification, development, testing or documentation of Palm Beach State applications must be familiar with this policy.

Manager Responsibilities – Palm Beach State managers responsible for developing applications must assure that each development team member has read and understood this policy and is given the proper resources to implement the controls outlined in this policy.

Information Technology Security Office (ITSO) – To support this policy, the ITSO must delegate an individual responsible for being the liaison with the application development teams. This individual must possess specific knowledge about the risks of application development and specific secure development practices.

Assigned Application Security Responsibility – Each application developed or acquired by Palm Beach State must have a designated individual responsible for the overall security of the system. This designation must be included as part of all system documentation used during design and development.

Training Requirements

Training Required - All employees involved in the coding of Palm Beach State business applications must receive training on secure coding principles.

Certification Required – At least one employee on each development team must receive a third-party certification in secure application development principles. The Manager responsible for application development will coordinate with the ITSO to select a proper certification and cost estimates.

Training Budget - Palm Beach State management will establish an annual budget for application security training, including the non-vacation time required to perform the training and certification by chose employees.

Application Acquisition

Security Requirements in RFP – All Palm Beach State Requests for Proposal (RFP) or Requests for Information (RFI) must include basic information security requirements established by the ITSO.

Application Specification Development

Sensitive Data Review – Each Palm Beach State application must include a review to identify any sensitive Palm Beach State data that will be processed as part of the application. A list of sensitive data types will be supplied by the ITSO and may include any of the following: Credit card numbers, Driver's License Numbers, Financial Information, Health Records, and other Personally Identifiable Information (PII).

Initial Application Criticality Classification – Each application built or acquired by Palm Beach State must have an initial application criticality classification. This rating will specify the overall level of security of the system, as well as the required recovery time for any system disruption.

Security Requirements – To reduce cost and maintain effective security, applications must be designed with security and privacy in mind. Each development specification document produced for Palm Beach State applications must include information security and data privacy requirements. Security and data privacy requirements must be identified as such within the specification document.

Security Department Review – The information security and data privacy requirements within the application specifications and design must be reviewed with a member of the ITSO.

Document Sensitivity – All specification, design, coding and testing documentation used in developing Palm Beach State applications must have an appropriate sensitivity label. By default, each document should be labeled for "CONFIDENTIAL: Internal Use Only".

Open Source and Third-Party Library Inventory – Part of the required documentation for each Palm Beach State application is a list of all third-party software packages used within the application. These include but are not limited to linked libraries, database applications, and encryption packages.

Encryption Algorithms – If any Palm Beach State application (1) uses encryption libraries and (2) will export the application across any international boundary,

the methods and types of encryption must be included within the documentation and reported to the Legal Department.

Logging of Security Events – All application code developed or purchased by Palm Beach State must produce a log of security-related events in an industry-standard format that supports monitoring by security audit programs.

Third Party Contractor Considerations

Approval of Personnel – Palm Beach State reserves the right of final approval for all contractors performing application development on Palm Beach State premises.

Policy Acknowledgement – All third-party contractors involved in the development of Palm Beach State applications must read and acknowledge understanding of the controls listed in this application security policy.

Restrictions on Third-Party Libraries – Only licensed software and in-house developed and authorized code (including government and contractor developed) shall be used on <system name(s)>. Public domain, shareware, or freeware software shall only be installed after prior written approval is obtained from the responsible development manager.

Restricted Disclosure - The contractor shall not publish or disclose in any manner, without the contracting officer's written consent, the details of any safeguards either designed or developed by the contractor.

Proof of License - The contractor shall provide proof of license for all software used to perform development of this application and for all third-party libraries included within the application.

Application Coding

Code Reviews – Palm Beach State application development teams must perform periodic reviews of source code for possible security and privacy flaws. Reviewers must possess special training in application security techniques or use a third-party authorized to review application security.

Source Code Labeling – All programming source code developed by Palm Beach State employees must be considered proprietary to the company and must be labeled as "Trade Secret."

Secure Coding Methods – All source code created by Palm Beach State developers must use secure coding methods approved by the development team.

Automated Tools – Palm Beach State will provide all development staff with access to automated vulnerability scanning tools which can assess source code for possible security flaws.

Code Obfuscation – All non-compiled, production source code used for web-based applications facing the public internet (such as PHP) must be “obfuscated” to hide the true business logic behind the application.

Source Code Management - All program source code used for Palm Beach State production systems must be stored in a secure source code management system with access controls approved by the ITSO.

Open Source Software

Conditions for Use of Open Source - Palm Beach State must not employ open source software for any production information system unless this software has been available for at least six months, is known to have been used and tested by at least fifty other organizations, and also is issued by a reputable organization known to have an on-going commitment to providing timely upgrades, patches, and fixes.

Open Source Software Widely Supported - Palm Beach State production computers must not employ open source software unless this software is known to have passed a rigorous security testing process undertaken by an independent and reputable third party. Additionally, this same software is known to be readily supported by a wide variety of technical consultants from different organizations.

Application Testing

Testing Data Sets – To maintain the security and privacy of its customers, Palm Beach State must limit the amount of sensitive data that gets duplicated, stored and transmitted. Applications that process sensitive Palm Beach State data (such as customer medical data, financial data, credit cards, etc.) testing must not use real customer data for testing purposes.

Sanitized Data Sets - Unless written permission is first obtained from the ITSO manager, all software testing for systems designed to handle private information

must be accomplished with "sanitized" production information. Sanitized information is production information which no longer contains specific details that might be valuable, critical, sensitive, or private.

Third-Party Testing – Palm Beach State must not employ any third party to test applications which process sensitive data unless test data has been sanitized to mask the true customer data.

Vulnerability Analysis and Testing

Vulnerability Analysis before Release – Before being released into production, all Palm Beach State business applications must undergo a vulnerability analysis and penetration test by either (1) a member of Palm Beach State staff trained under this discipline, or (2) a trusted third-party.

Regular Vulnerability Analysis for Web-Based Production Applications – All Palm Beach State web applications that are available to the public internet must have periodic monitoring for vulnerabilities by a trusted third-party. Vulnerability analysis must be based on, at a minimum, the most recent list of common vulnerabilities available from Open Web Application Security Project (OWASP).

Special Requirements for PCI-DSS

PCI Identification Required – Any Palm Beach State application that will process, transmit or store credit cards must be clearly identified within the application development lifecycle as being subject to the requirements of the Payment Card Industry Data Security Standard (PCI-DSS).

Quarterly Vulnerability Scan – Any Palm Beach State application that will process, transmit or store credit cards must be subject to a vulnerability scan approved by the ITSO. This scan must be done at least quarterly.

Web Application Firewall – Any Palm Beach State application which can be accessed via the internet must include an application layer firewall approved by the ITSO.

Application Decommission and Disposal

Information Preservation – Before any Palm Beach State product applications are taken out of production, a final backup of all sensitive production data must be preserved for at least three (3) years. Backup media that store this production

Application Development Policy

data must contain a classification label which matches the highest (most sensitive) classification of the data being stored.

Media Sanitization – After any Palm Beach State application is taken out of production, all media which stores application code or data must be sanitized according to Palm Beach State media sanitization guidelines.

Hardware/Software Disposal – Hardware and other media which contained production application code or data must not be disposed or resold unless it has both (1) been properly sanitized and (2) has been approved by the ITSO.

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	6/30/2009		