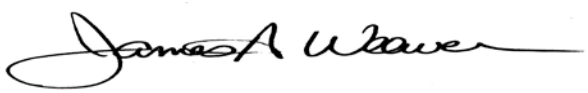
COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF PUBLIC WELFARE

INFORMATION TECHNOLOGY STANDARD

Name Of Standard: **Mobile Application**	Number: **STD-ENSS029**
Domain: **Security**	Category:
Date Issued: **09/07/2012**	Issued By Direction Of:
Date Revised:	 James Weaver, Dir of Div of Tech Engineering

Abstract:

The purpose of this standard is to describe the department's minimum expectations for secure mobile application development, deployment and threat mitigation.

To better serve the citizenry and workforce, the Department of Public Welfare (DPW) has embarked on a strategic initiative to define and operationalize their mobile application architecture. This standard develops a set of guidelines that define the foundation for mobile based solutions to support potential citizen-facing mobile applications.

These guidelines should be applied based on the sensitivity of the data the mobile application is processing. These guidelines should be applied based on the following factors:

- The level of risk (defined below) based on the classification of data handled
- Business considerations of usability and the extent of reach and adoption desired

The security control guidelines have been defined to make the best use of DPW's existing security technology, processes and tools.

The following activities are to be performed to improve mobile application security:

Mobile Risk Assessment

A risk assessment of every mobile application should be carried out. The risk assessment should include risk cataloguing and categorization in order to develop required controls and mitigation measures.

The objective is to provide the business owners with the necessary information to make an informed decision on an acceptable level of risks and controls.

Mobile Secure Code Review

A review of the mobile application source code aiming to identify insecure coding practices and document identified vulnerabilities.

The objective is to identify insecure coding techniques and vulnerabilities that could lead to security issues.

Mobile Application Security Baseline
A review of the entire mobile application from the perspective of documented security controls and configurations, should be conducted every 2 years. Appropriate revisions should be made to the application configuration baseline to account for new best practices and industry recommendations.

The scope of the Mobile Application Security Standards is limited to code that is developed by the application teams only and will only be undertaken in the development and test environments. The Department will undertake the holistic vulnerability and penetration testing aspects that include the infrastructure, network, and other components that make up the production infrastructure. This standard complements other product and deployment standards already in place by the Department such as the use of the Unified Security solution for authentication and authorization.

General:

Mobile Application Security Standard applies to the Department of Public Welfare ("Department") mobile application architecture developed by the Department or contractors. The requirements outlined in this document are the minimum considered adequate to identify potential vulnerabilities due insecure coding practices, insufficient design and inadequate security controls.

Standard:

Mobile Risk Assessment

The DPW information security risk management process requires every mobile application to be assessed for risk, including risk cataloging and categorization, in order to develop required controls and mitigation measures. This process enables the business owners to make informed decisions on acceptable levels of risk and control.

The risk assessment should be completed by the application development team as part of the application design process. See the Risk Assessment Questionnaire Standard for details on conducting this activity.

Additionally, the following is the summary of risk level classifications, specific to mobile applications, based on the sensitivity of the data:

Risk level	Rationale	Examples
Low Risk Applications	Sections of mobile web application which provide access to publically available information	• Public announcements • Informative articles • Department's contact information
Medium Risk Applications	Sections of mobile web application which provide access to a user's or a department's non-public information but not related to the user's PHI, child abuse information and other sensitive data identified in that application.	• User's application or case status (e.g.: Pending, Accepted, Rejected) • Appointment date, Attendance tracking
High Risk Applications	Sections of mobile web application which provide access to a user's or a department's non-public information related to the user's PHI, child abuse information and other sensitive data identified for that program.	• User's application or case details • Subsidy values (dollar amounts) • SSN, Medicare/Medicaid ID, driver's license, FEIN and financial account numbers with PIN

Mobile Secure Code Review

Secure code review is to be performed during the development phase of the application development lifecycle. Secure code review serves to identify insecure coding techniques and vulnerabilities that could lead to security issues. This activity will reinforce the need to adhere to secure coding principles to development teams and is intended to identify issues as early as possible in the software development life cycle.

Secure coding principles would include, but are not limited to, the following:

- Input Validation
- Output Validation
- Authentication
- Authorization
- Session Management
- Code Access Security
- Configuration Management
- Data Access Control
- Error & Exception Management
- Auditing & Logging
- Data Encryption

All developed mobile code must meet the following minimum security controls guidelines based on the risk classification:

Security control	Guidelines	Mobile Web Applications Risk Classification			DPW Managed Devices
		Low	Medium	High	
User authentica-tion	Use the existing DPW's IAM infrastructure for user's authentication to the mobile web application[1, 2]	N/A	Single factor (username +password)	Multi factor (two or more, based on the risk)[3]	[TBD]
HTTP(S)	Use of SSL v3/TLS v1.2 over HTTP using at a minimum 128-bit session key encryption	Recom-mended	Yes		[TBD]
User registration	Allow user registration in the mobile web application	N/A	Yes, challenge-response test is required (Captcha)		[TBD]
Session timeout	Predetermined time of inactivity after which the server should require the user to provide login credentials	N/A	5-10 min	< 5 minutes	[TBD]
Session concurrency	Allow for multiple (concurrent) sessions	N/A	No		[TBD]
Last login	Indicate the user's last login time.	N/A	Yes		[TBD]
Manual logout	Provide a way for a user to log out of the application (with a button or link)☐	N/A	Yes		[TBD]
Full website	Restrict access to	No	Yes		[TBD]

Security control	Guidelines	Mobile Web Applications Risk Classification			DPW Managed Devices
		Low	Medium	High	
access restriction	the full version of the website from a mobile device.				
Device registration	Require registering user's mobile device prior to accessing the user's or department's non-public information☐	No	Recom-mended	Yes	[TBD]
Disclaimer	Inform the user that the information requested is being rendered on a mobile device and if the user wants to proceed	N/A	Yes		[TBD]
Privacy policy	Provide a privacy policy (user accepts each time when visiting the mobile website)	N/A	Yes		[TBD]
Audit logging	Leverage DPW's audit logging policy and existing controls used for the desktop version.	N/A	The log should contain the device type and device location (if GPS tracking is enabled and used for the solution).		[TBD]
Vulnerability testing	Leverage existing DPW's standard for security vulnerability testing and code review (ENSS020).	Yes			[TBD]
Code review	Leverage existing DPW's standard for security vulnerability testing and code review (ENSS020).	Yes			[TBD]
Browser side cache control	Use HTTP headers to control the browser (client) cache	Allow browser cache	No cache		[TBD]
Downloadable data	Allow content to be downloaded in form of a PDF and/or other office files (including but not limited to Open Office, Quick Office and Microsoft Office files)	Yes	Requires review by the DPW Security.		[TBD]
Track device location using device GPS functionality	Indicates if a mobile device location can be tracked. Device tracking requires the privacy policy to be	No	Yes	Yes. Block access to mobile web application if location can't	[TBD]

Security control	Guidelines	Mobile Web Applications Risk Classification			DPW Managed Devices
		Low	Medium	High	
	shown to the user each time the user accesses the mobile web application.			be established.	
Local storage	Indicates if the mobile web application can use the mobile device local data store (such as SQL Lite in Apple IOS).	Yes	Yes - PII data should not be stored		[TBD]
PII catalog	Update the Department's PII catalog for content/files downloadable through the mobile web application.	Yes			[TBD]

Mobile Application Security Baseline

The Department expects to establish a baseline of the security posture of the applications on a periodic basis (once every three years). As part of the baseline assessment, vulnerability testing should be performed on the entire web application and related services using automated tools and manual techniques.

At the end of the application security baseline assessment, the application stakeholders are expected to perform a business impact analysis for the identified vulnerabilities. The report detailing the vulnerabilities, the security severity, business impact and the corresponding mitigation plan should be submitted to the Security Team Manager at the Bureau of Information Systems (BIS)/Department of Technology Engineering (DTE). Upon consensus of the vulnerability mitigation plan, the mitigation plan should be documented and managed by the application development team management similar to any other application defect.

Exemptions from this Standard:

An application development team that is unable to comply with this standard must discuss any exemption request with the Departments' Chief Information Security Officer (CISO).

Refresh Schedule:

All standards and referenced documentation identified in this standard will be subject to review and possible revision annually or upon request by the DPW Information Technology Standards Team.

References:

1. GEN-SEC019A: Data Classification Quick Reference Guide and Data Classification Standards
2. ITB-PRV001 Commonwealth of Pennsylvania Electronic Information Privacy Policy
3. STD APP001S: Application Security Standards & Policies
4. Open Web Application Security Project: http://www.owasp.org
5. NIST SP800-64: Security Considerations in the System Development Life Cycle (Revision 2)

Standard Revision Log:

Change Date	Version	Change Description	Author and Organization
09/07/2012	1.0	Mobile application	Clifton Van Scyoc