Lebanese American University

Information Security Regulations

Application Development Regulations

Last Updated: May 2017
Version 1.2

Overview

LAU develops and purchases a variety of application software as part of ongoing business operations. These are critical to LAU's business and often contain sensitive information. To reduce the risk of accidental disclosure of sensitive information, and to protect LAU information assets, all LAU applications must be developed with the highest levels of data security and privacy.

Purpose

These regulations define LAU requirements for the secure development, testing and deployment of applications developed in-house or by third parties.

Scope

These regulations apply to all applications that fall under the umbrella of LAU IT Department.

Regulations

Security Requirements

To maintain effective security, applications must be designed with security and privacy in mind. Each development specification document produced for LAU applications, RFP or RFI, must include information security and data privacy requirements that 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 Information Security Department.

Open Source and Third-Party Library Inventory

Part of the required documentation for each 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.

Logging of Security Events

All application code developed or purchased by LAU must produce a log of security-related events in an industry-standard format that supports monitoring by security audit programs.

Training Required

All employees involved in the development of LAU business applications must receive training on secure coding principles.

Regulations Acknowledgement
All third-party contractors involved in the development of LAU applications must read and acknowledge understanding of the controls listed in this application development regulations document.

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.

Source Code Labeling
All programming source code developed by LAU employees must be considered proprietary to LAU.

Conditions for Use of Open Source
LAU 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 passed a rigorous security testing process undertaken by an independent and reputable third party, and also is issued by a reputable organization known to have an on-going commitment to providing timely upgrades, patches, and fixes.

Vulnerability Analysis before Release
Before being released into production, all LAU business applications must undergo a vulnerability analysis and penetration test by either a member of LAU IT Security Department or a trusted third-party.

Regular Vulnerability Analysis for Web-Based Production Applications
All LAU 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).

Web Application Firewall
Any LAU application which can be accessed via the internet must include an application layer firewall where applicable.

Change Control Procedure
All significant changes to critical IT systems must be communicated through the IT Change Management Application.

Separation between Development, Test and Production Environments
Development, test and production environments should be separated and none of them can co-exist on the same server.

Developers Access
Developers should have full access to the development environment and only read access to the test and production environments unless absolutely required and after securing the approval of the IT director concerned.

Transfer Files between Development, Test and Production Environments
Transfer of files between development, test and production environment should be done by the system administrators or automated where applicable, and it should be a one-way transfer. Files can be transferred only from development to test and from test to production environments. Files

cannot be transferred from test to production environment unless the user acceptance test was passed successfully.

Documentation Kept Up-to-date

Documentation must be kept up-to-date during all the life cycle of the application.