Responsible Use of University Computing Resources Policy Document

Web/Database Application Development

and Verification Testing Policies

1. Purpose

Montclair State University's Information Technology Division (IT) has adopted a web application development platform consisting of specific operating systems, web servers, databases, and programming tools that can be used to host web applications developed in-house or by outside contractors. The purpose of this document is to define the components of the University's supported web development platform, coding standards, and testing and approval process so that applications can be developed in a manner consistent with accepted interoperability and security practices and be fully compatible and supportable in our environment.

2. Scope

Any University division, department, or individual that develops applications that will run on IT or departmental computing platforms. This includes both web-based and traditional client/server based applications.

3. Acceptable Technologies

In general, in-house developers or outside contractors hired to develop custom web-based applications for use on IT supported servers should develop those applications using **open standard** protocols, languages, and tools. IT defines open standard to mean:

"A technology whose specifications are published and freely available, (ex. HTML, XML, PHP, Java) and sufficiently detailed such that applications written according to the specification will work with any other software or platform designed for compliance with said specification."

The list of acceptable open-standards technologies that are supported by IT include but are not limited to:

- Java / JSP / JavaEE (Java is IT's preferred platform for all application development)
- PHP 5 or later.
- W3C standards-compliant HTML, XHTML, CSS, DHTML, XML, DOM.
- Javascript/ECMAScript
- Python
- Ruby
- SSL/TLS
- Apache/Tomcat
- SQL standards such as SQL-92, 99, or 2003 (vendor-specific SQL extensions should be avoided)

Note: Web developers intending to use any technologies other than those listed above must consult with IT before any development work begins. IT cannot guarantee application compatibility with our existing infrastructure if non-supported technologies are used for development or deployment.

4. Platform and Functionality Considerations

To ensure application compatibility within MSU's campus computing infrastructure, web application developers should keep the following in mind:

- Production web applications servers at MSU primarily use Apache 2.x on Linux, Solaris and Windows Server platforms.
- Microsoft's IIS web server and/or Active Server Pages (ASP) technologies are supported only when required by third party applications.
- While IT primarily uses Apache Tomcat, all Java web application code must be written to run in any J2EE 6 or higher-compliant web application container architecture.
- Microsoft SQL server is supported by IT for traditional client-server database applications. However, the preferred database platforms for web-based applications are Postgres, MySQL, and Oracle 11g.
- Web-based applications must support recent versions of all popular web browsers, including Mozilla Firefox 17 or higher, Internet Explorer 10 or higher, and Safari 5 or higher. Adhering to W3C web standards is the best way to ensure this compatibility.
- Any user authentication mechanisms must provide an encrypted (SSL) HTTPS connection for the login screen to avoid transmitting username and password information in plain text. IT can provide SSL certificates upon request.

- Authentication mechanisms that utilize MSU NetIDs must be done via an encrypted, anonymous bind to the campus LDAP server. Where applicable, user authorization should be handled via LDAP groups.

- Any file transfer operations, SQL queries, or directory service lookups must occur over a secure channel such as SSL, SFTP, or SCP.

5. Application Verification Testing and Development Lifecycle

- Applications should be designed based on the platforms, tools, and data connectivity guidelines presented in this document and other related University policy documents such as Safeguarding Sensitive and Confidential Information and Secure Directory Services Access for User Authentication and Authorization.

- Functional requirements for applications should consider all appropriate University policies, industry guidelines, and state and federal regulations for secure access, handling of sensitive data, and protection of personally identifiable information (PII) or financial records. Examples include HIPAA, FERPA, and PCI-DSS.

- Whenever possible, application development will be performed in a secure 'dev' or 'test' environment that is isolated from the Internet and may have limited or no access to the University's production server farm and campus network.

- Prior to moving an application from the dev/test environment to production use, the application will be scanned by IT's Systems and Security Group for known security vulnerabilities using automated tools such as WebInspect, AppScan, or other commercial and open-source utilities. Application developers are encouraged to request periodic security scans during the development process (i.e. at each milestone of the project) to pro-actively address security vulnerabilities and reduce the likelihood of issues arising during the final pre-production scan.

- When the pre-production application scanner has been completed, the application will be moved into the appropriate production environment and any required external firewall rules for remote communication will be enabled.

- IT's Systems and Security Group will periodically re-scan applications that are in production use to ensure that they are not vulnerable to new attack methods.