29.01.99.L1.04 Application Development Security

Approval date: 03/28/13
Revision date: 01/24/13
Next scheduled review date: 01/24/15
Author: Office of Information Technology

**Standard Administrative Procedure Statement**

**General**
Application development security measures must be taken throughout an application’s life cycle in order to build more secure and robust applications. When a web application’s design begins, it is essential to apply threat risk modeling; otherwise, resources, time and money will be consumed on useless controls that fail to focus on the real risks.

Texas A&M International University (TAMIU) has adopted Microsoft’s threat modeling process to address the unique challenges facing web application security. This model is simple to learn and adopt by designers, developers, code reviewers, and the quality assurance team.

**Applicability**
This SAP serves as a framework for developing, deploying and maintaining secure applications. In order to incorporate security into the application life cycle, this SAP can be used together with TAMIU’s 29.01.99.L1.21 System Development and Acquisition SAP.

This SAP is intended for all developers, security testers and system architects developing and/or administering applications to process TAMIU data.

**Definitions**

**DREAD**: A classification scheme for quantifying, comparing and prioritizing the amount of risk presented by each evaluated threat. The DREAD acronym stands for: Damage Potential, Reproducibility, Exploitability, Affected Users and Discoverability.

**Information Resources (IR)**: Any computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, tablets, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), smartphones, telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it includes the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.
**Information Resource Owner:** an entity responsible for:

- a business function; and,
- determining controls and access to information resources supporting that business function.

**Information Security Officer (ISO):** Person responsible to the executive management for administering the information security function within the University. The ISO is TAMIU’s internal and external point of contact for all information security matters.

**Office of Information Technology (OIT):** The name of the University department responsible for computers, networking and data management.

**Software:** A computer program which provides instructions to computer hardware. System software such as Windows or MacOS, operate the machine itself. Application software such as spreadsheet or word processing programs provides specific functionality.

**Standard Operating Procedure (SOP):** Set of detailed instructions for performing a specific process.

**STRIDE:** A classification scheme for characterizing known threats according to the kinds of exploits that are used (or motivation of the attacker). The STRIDE acronym stands for: Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, and Elevation of privilege.

---

### Procedures and Responsibilities

#### 1. Application Development Standards

The following list of procedures should be applied to the development of applications that process University data:

1.1 Application Developers must complete a threat risk model using the Microsoft Threat Modeling Process.
   
   The threat risk modeling process consists of five steps:
   
   1.1.1 Identify Security Objectives
   
   1.1.2 Survey the Application
   
   1.1.3 Decompose it
   
   1.1.4 Identify Threats
   
   1.1.5 Identify Vulnerabilities (STRIDE and DREAD)

   Developers should use the Threat Risk Modeling SOP to accomplish this process.

1.2 Applications should validate input properly to restrict unexpected characters. This will minimize the risk of attacks performed by embedding malicious strings in form fields, cookies and HTTP headers. Examples of these attacks include, but are not limited to, cross-site scripting (XSS), SQL Injection and buffer overflow attacks.

1.3 Applications should execute proper error handling and display appropriate messages so as not to provide detailed system information to users, impair the system, or deny service.
1.4 Identity spoofing, elevation of privileges, password cracking and unauthorized access must be reduced.

1.5 Authentication and session management must not be vulnerable to session hijacking.

2. **Application Administration Standard**

2.1. OIT needs to perform a certification of the system before the application goes to production.

2.2. The Information Security Officer must always have a full inventory of all web applications.

2.3. Security scans on the applications must be performed before deployment. Reports will be sent to the system owner with the identified vulnerabilities for corrective action.

2.4. Security scans must be performed at least annually after deployment in order to identify vulnerabilities.

<table>
<thead>
<tr>
<th>Related Statutes, Policies, Regulations, Rules or Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAC 202.75 Security Standards for Institutions of Higher Education</td>
</tr>
</tbody>
</table>

---

**Appendix**

**Improving Web Application Security: Threats and Countermeasures**
OWASP Top Ten Project [http://www.owasp.org](http://www.owasp.org)

<table>
<thead>
<tr>
<th>Contact Office</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Office of Information Technology</strong></td>
</tr>
<tr>
<td>Hotline: (956) 326-2310</td>
</tr>
<tr>
<td>Killam Library 257</td>
</tr>
<tr>
<td><strong>Information Security Officer</strong></td>
</tr>
<tr>
<td>Cuauhtemoc Barrios</td>
</tr>
<tr>
<td><a href="mailto:cbarrios@tamiu.edu">cbarrios@tamiu.edu</a></td>
</tr>
<tr>
<td><strong>Office Hours</strong></td>
</tr>
<tr>
<td>Monday - Friday: 7:30 AM - 6:00 PM</td>
</tr>
<tr>
<td>Saturday - Sunday: Closed</td>
</tr>
<tr>
<td><strong>ITSecurity Group</strong></td>
</tr>
<tr>
<td><a href="mailto:itsecurity@tamiu.edu">itsecurity@tamiu.edu</a></td>
</tr>
</tbody>
</table>