Securing Public Websites

Introduction
The World Wide Web is a phenomenal communication and marketing tool that has been whole-heartedly embraced by UTMB. Its use has promoted our healthcare, academic and research initiatives throughout the world, helping us retain our competitive edge over other academic healthcare institutions. However, if we are not conscientious with the way we configure and operate our public web services, it could have a negative effect on our institution as a whole. Improperly configured or operated web services threaten the confidentiality, integrity and availability of our information. Cyber security threats are in many ways, similar to physical threats, i.e., fraud, theft, vandalism, etc., with one caveat, it is much more dangerous. Cyber security threats have three distinct advantages for the criminal: increased efficiency; action at a distance; and rapid technique propagation.

Increased Efficiency – With the computing power of today and the availability of high-speed data connections, cyber attacks are usually automated and fast. They go from system to system in an efficient manner looking for weaknesses to exploit. Once a weakness is discovered, it’s quickly exploited, exposing any confidential information, which the system may store or process. At that point, cyber criminals are automatically notified of the exploited system, so that data can be retrieved and reviewed for profit potential.

Action at a distance – While the World Wide Web puts UTMB on the world stage for all to see and admire, It also makes our Internet accessible services susceptible cyber attacks from anywhere in the word.

Rapid Technique Propagation – Because of automation and high speed connections, cyber attacks are easily and efficiently propagated throughout the internet. This makes it difficult for organization to take a reactionary stance. Over the course of realizing that an attack is in progress, developing and deploying countermeasures, hundreds, if not thousands of system could have already been compromised.

To guard against these threats, it is essential that all web services administrators take proactive steps to secure these systems so that our patients, students, faculty, staff and associates are confident that the information they entrust to us is protected from malicious and criminal activity.
Securing Public Websites, Continued

Purpose
This document sets minimum baseline security requirements for new and existing web services systems. It provides instruction on how to design, implement and maintain publically accessible websites that are owned, operated and/or controlled by UTMB.

Audience
All UTMB faculty, staff and students, who operate, maintain, control and/or administer web services platforms are required to adhere to this practice standard. Any deviation (security degradation) from this standard requires approval from the Office of Information Security. Exception can be requested at http://www.utmb.edu/infosec.

It is assumed that web services personnel possess a basic knowledge of web development and website administration.

Implications
- All personnel who support publically assessable websites shall ensure that they are secured in accordance with this practice standard.
- Publically assessable websites shall be approved by department prior to being assessable from the internet.
- Network and Security Services shall conduct vulnerability scans of all publically assessable web sites on a annual basis. Vulnerability reports will be made available appropriate web developers and system custodians for the purpose of remediation.
- Pursuant to pertinent policy and practice standards, the Office of Information Security will, at its discretion, disable any unauthorized or non-compliant website that it discovers on the UTMB network.

Sensitive Digital Data Management
Sensitive Digital Data, as defined by UTS 165, includes social security numbers, Protected Health Information (PHI), Sensitive Research Data, digital Data associated with an individual and/or digital Data protected by law. Sensitive digital Data must be secured and protected while at rest (electronic storage on a hard drive, digital or optical media), mobile (laptop, PDA or flash drive) and in transit (via email or the Internet).
## Securing Public Websites, continued

<table>
<thead>
<tr>
<th>Practice Standards</th>
<th>ADMINISTRATIVE STANDARDS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All publically assessable websites shall reside on the UTMB Content Management System (CMS).</td>
</tr>
<tr>
<td></td>
<td>Prior to allocating space on CMS, websites must be approved in writing by the department Chair, Administrator or equivalent.</td>
</tr>
<tr>
<td></td>
<td>Prior to publishing a website external to UTMB, the Office of Information Security shall scan it for vulnerabilities. Once any identified significant vulnerabilities have been remediated; the office of information security will certify the site and approve it for external publishing.</td>
</tr>
<tr>
<td></td>
<td>All publically assessable websites shall be scanned for vulnerabilities on an annual basis. Any critical vulnerabilities identified shall be remediated within one business day. All other vulnerabilities shall be remediated within 10 business days. Failure to remediate vulnerabilities within the allotted time may result in a disruption in web services. Additional scans may be required, as new vulnerabilities or potential exploits are identified.</td>
</tr>
</tbody>
</table>

## WEB CONTENT SECURITY

- No confidential or personally identifiable information (PII) shall be stored on publically assessable website.
- All confidential and/or personally identifiable information that is assessable via the Internet shall reside in a repository that is physically or logically separated from the content management system and is adequately secured behind an institutional firewall.
- Web sites that require an individual to enter confidential and/or personally identifiable information in a web-based electronic form shall use a secure socket layer session or equivalent technology to encrypt the data.
- Access to confidential or personally identifiable information shall be controlled using a UTMB managed Lightweight Directory Authentication Protocol, Active Directory or UT System Identity Management Federation.
- No pages within a web application that requires user authentication shall be assessable without executing the logon process.
- Web application that require user authentication shall incorporate a timing mechanism and log users out after 10 minutes of inactivity.
- After three failed logon attempts, the user will be redirected to an information/warning page.
Wireless Access, continued

**Practice Standards (con’t)**

**CONFIGURATION SECURITY**
- All external scripts and programs executed as part of the web server content, i.e., CGI, ASP etc, shall reside in a single dedicated directory.
- To guard against SQL injection, developer shall ensure that mechanism’s are in place to validate user input.
- Persistent cookies should not be used.
- No directories shall have both write and execute permission.
- Source code for all third party scripts and executables shall be verified prior to use.
- Dynamically created Web pages shall be reviewed for dangerous metacharacters.

**PRIVACY**
- Public web sites will not collect personally identifiable information about individuals except when individuals intentionally provide such information in a question, transaction, on a web form or other web-based communication sent to the university.
- At a minimum, the home page of all public web sites will include a link to UTMB’s privacy policy, located at [http://www.utmb.edu/site-policies/privacy.asp](http://www.utmb.edu/site-policies/privacy.asp).

**WEB ACCESSABILITY**
- Public web sites must be accessible to all users and be designed and developed in accordance with the standards as outlined in [Title 1, Part 10, Chapter 206.70 of the Texas Administrative Code](http://www.utmb.edu/identity/web/).

**BRANDING**
- All public web sites must be developed using a UTMB supported institutional web site template located at [http://www.utmb.edu/identity/web/](http://www.utmb.edu/identity/web/).

**Disciplinary Actions**
Violation of this policy may result in disciplinary action which may include termination for employees; a termination of employment relations in the case of contractors or consultants; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTMB IR access privileges, civil, and/or criminal prosecution.

**References**
- Texas Administrative Code Chapter 206.70
- UTMB Web Privacy Statement
- UTMB Presidents Memo on Branding, Dated September 23, 2010
- NIST Special publication 800-44