Web Hosting Policy [1]

Version 1.0

Authority

Duke University Chief Information Security Officer
Duke University Vice President for Public Affairs and Government Relations

Introduction

Duke has a longstanding practice of using websites to communicate, share information and transact business with internal and external constituents. Over the years, Duke’s web presence has grown to include:

- Institutional websites including www.duke.edu [2]
- Websites involved in e-commerce or other sensitive data
- School, center, institute and departmental websites (such as trinity.duke.edu)
- Individual or project-oriented websites

These websites can be hosted at Duke or with external hosting companies. Website support responsibilities may range from full support by a Duke web hosting group or a third party to best effort by a faculty, student or staff member.

Duke websites present a very viable risk to the university and can provide an avenue of attack against other Duke systems. There is a direct relationship between website compromises and unpatched web environments and associated servers. In an effort to improve the security of all Duke’s websites, the IT Security Office (ITSO), Office of Information Technology (OIT) and Office of Marketing and Strategic Communications (OMSC) have developed guidance and options for those managing websites at Duke.
Scope

This policy applies to Duke-affiliated websites and web applications maintained either on the Duke network or with a third-party (external) hosting provider and to internal or third-party developers responsible for building or maintaining Duke websites.

Policy

Website Categories

Websites at Duke are grouped into four general categories. OMSC, in consultation with the website owner and the ITSO, will determine categorization of a particular website.

1. **Institutional**: Websites that are highly visible, provide institutional services or carry a higher level of scrutiny (e.g., [www.duke.edu](http://www.duke.edu) and main navigation/landing pages).

2. **Sensitive Data**: Websites that are dealing with sensitive data in some manner (e.g., credit card processing, protected research data).

3. **School/Department**: Websites that are more focused on a particular group (e.g., a school, department, institute).

4. **Individual**: Websites that have a smaller audience or smaller scope by nature (e.g., a personal or course website, or a website set up to provide details on a research project) and are not hosted by central services.

A listing of institutional and sensitive websites will be maintained by OMSC and the ITSO on the Duke Style Guide website.

The following table outlines the requirements for each category of websites:

<table>
<thead>
<tr>
<th></th>
<th>Institutional</th>
<th>Sensitive Data</th>
<th>School/Department</th>
<th>Individual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosted by</td>
<td>OIT, DHTS, approved 3rd party</td>
<td>OIT, DHTS, Protected Network or approved 3rd party</td>
<td>OIT, DHTS, School, approved 3rd party</td>
<td>Any</td>
</tr>
<tr>
<td>Developed By</td>
<td>DHTS, DWS, School, approved 3rd party</td>
<td>Any</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------</td>
<td>---------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit</td>
<td>Conducted annually</td>
<td>Annual sample of websites</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Typical Patching Requirement*</td>
<td>Within 72 hours</td>
<td>1 week</td>
<td>2 weeks</td>
<td></td>
</tr>
<tr>
<td>Compromise Quarantine**</td>
<td></td>
<td>Immediate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Acceptance</td>
<td>Senior University Leadership</td>
<td>Chair/Dean/VP</td>
<td>Individual</td>
<td></td>
</tr>
<tr>
<td>Maintenance Contract &amp; Recovery</td>
<td>Required contract defining ongoing maintenance responsibility by vendor, and recovery costs/timelines; recovery requiring institutional intervention will be tracked and monitored and may incur costs</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Patching timeframes may be accelerated at the ITSO’s discretion for more severe exploits. In those cases, the ITSO will communicate accelerated patch requirements via campus communication channels including the security liaisons email list at security-liaisons@duke.edu

**A compromised website will be quarantined by the ITSO (i.e., taken off the public-facing Internet) until the compromise is addressed and the ITSO authorizes the website’s reinstatement. A website may also be quarantined if patching requirements are not met.

**Website Development and Hosting**

Duke websites in the Institutional, Sensitive or School/Department categories must be hosted and/or developed by OMSC-approved vendors who have met Duke standards for security and design.

Many pre-approved options are available to the Duke community for developing, hosting and managing websites, including:

- Development and hosting by Duke Web Services (http://webservices.duke.edu/) and the Office of Information Technology (OIT), which provides a centralized web hosting environment that includes complete management of the web sever and content (https://oit.duke.edu/enterprise/infrastructure/Virtual%20Server%20Hosting...
- Development and hosting by DHTS Web Services ([http://webservices.dhts.duke.edu/](http://webservices.dhts.duke.edu/))
- Development and hosting by school-managed web hosting and development services, in conjunction with local IT support.
- Partnering with an approved third-party hosting provider or web developer, in consultation with the Office of Marketing and Strategic Communication (OSMC).
- Self-service development and administration (with options outlined below, including sites residing on a school/department or OIT-managed web server and/or using a service such as Duke WordPress ([https://sites.duke.edu](https://sites.duke.edu)).

Websites often have multiple layers with different responsibilities at each layer. Layers may include the operating system (OS), web server software, and a content management system like Drupal or WordPress (CMS). Websites at Duke are expected to have an identified administrator at all layers. A website administration (referred to below as the customer) may include the data or content owner or the individual responsible for coordinating the implementation of the website.

The following table outlines responsibility for ongoing patching and maintenance of each layer/component of a Duke website:

<table>
<thead>
<tr>
<th>If hosted by:</th>
<th>Operating System</th>
<th>Web Server Software</th>
<th>Content Management System</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>OIT (with support option)</td>
<td>OIT web hosting</td>
<td>OIT web hosting</td>
<td>Customer or hired developer</td>
<td>Customer</td>
</tr>
<tr>
<td>3rd-party vendor (e.g. hosting.com)</td>
<td>Customer</td>
<td>Customer</td>
<td>Customer or hired developer</td>
<td>Customer</td>
</tr>
<tr>
<td>Schools/departments</td>
<td>OIT</td>
<td>OIT</td>
<td>School IT or Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>Sites @ Duke</td>
<td>Customer</td>
<td>Customer</td>
<td>Customer</td>
<td>Customer</td>
</tr>
<tr>
<td>Individual</td>
<td>Customer</td>
<td>Customer</td>
<td>Customer</td>
<td>Customer</td>
</tr>
</tbody>
</table>
When a developer is hired to build a website, the contracting unit must ensure that arrangements have been made to provide ongoing support, especially for addressing security vulnerabilities and patching of the content management system.

Hosting or developing a website with a 3rd party outside of Duke does not absolve the Duke website owner of their responsibility to keep the website patched.

Requirements for Website Owners / Administrators

Duke websites must follow the requirements documented in the Duke Web Security Standards [11]. In particular, website owners and administrators should focus on the following requirements during initial setup and for ongoing maintenance:

- Use only supported and up-to-date software that is actively maintained by an established, reputable vendor (e.g., Microsoft, Oracle) or open-source community (e.g., Drupal, WordPress).
- Use Duke’s Shibboleth service for website logins unless prior approval has been granted by the ITSO. For information on implementing Shibboleth, visit https://idms-web.oit.duke.edu/spreg/sps [12]. If, for some reason, you cannot use Duke’s Shibboleth service to authenticate users, ensure that you have configured your authentication mechanisms to occur over HTTPS and file an exception with the ITSO.
- Monitor the various security lists for software installed on or supporting the website to receive notification of security updates.
- Apply security updates to the operating system, web server (e.g., Apache), and CMS (e.g., Drupal) as they become available and in compliance with the patching timeline requirements.
- Apply the hardening standards from the Duke Web Security Standards [11]. If a site uses a technology not included in the Duke Standard, the site administrator is responsible for working with the ITSO to determine and follow appropriate security measures.
- Those running a Drupal or WordPress site will be required to install a Duke-developed security plugin, which will report the CMS and plugin versions to the site owner and ITSO. For installation guidelines, consult the Duke Web Security Standards wiki [13].
- Any work being done through a third-party or internal organization requires a minimum service-level agreement of 10 hours per year. Due to the changing nature of the web and the need for version and security upgrades on our preferred platforms, site owners need to ensure there is budget and calendar time available for application of security patches in compliance with the stated timeframe requirements.

Requirements for External Vendors

External vendors must be registered with Duke’s Office of Marketing and Strategic Communications (see the Style Guide at https://styleguide.duke.edu/ [3] for details on process). In addition, all external vendors must:

- Go through a vendor risk assessment [14] with the IT Security Office.
• Comply with PCI requirements if taking credit card payments (see below).
• Include specific security and patching requirements in contract and/or a Service Level Agreement (SLA).
• Include Duke’s Data Security Agreement (DSA) in the contract.
• Participate in monthly vulnerability scanning through the ITSO and remediate the issues reported in compliance with the patching timeline stated above.

Websites Processing Electronic Payments (PCI Compliance)


• Be hosted at Duke or with a hosting provider meeting PCI’s Level 1 compliance requirements [17].
• Utilize DukePay [18] (delivered via CyberSource).
• Have a plan to address the requirements for website administration and external vendors.
• Register the website with the E-Commerce office for quarterly PCI vulnerability scanning and remediate the issues reported in compliance with the patching timeline stated above.

Compliance

Any person who is responsible for a Duke-related website consents to the policies outlined above. Website owners have a responsibility for the security of their websites. Violations of the policy may result in the loss of usage privileges, administrative sanctions (including termination or expulsion) as outlined in applicable Duke University disciplinary procedures. These policies are subject to review and audit by Duke’s Office of Internal Audits.

Responsibilities

All owners and administrators of Duke websites are responsible for implementing the policies described in this document.

Review Frequency: Annually
Updated: 14-Aug-15