**General Description**

**Purpose:**
Vulnerabilities within networks, software applications, and operating systems are always a threat, whether due to server or software misconfigurations, improper file settings, or outdated software. Vulnerability management is a critical component of the university’s information security program and essential to reducing potential financial, reputational, and regulatory risks. This policy establishes a framework for identifying, assessing, and remediating vulnerabilities on devices connected to Trinity University’s networks.

**Scope:**
This policy applies to all Trinity University-owned and managed devices and networks, including but not limited to computer workstations, servers, network switches and routers, networked printers, scanners, copiers, and digital telecommunications.

Vulnerability scanning is limited to reviewing IT system and application configuration and does not include review of content found in email or digital documents.

**Policy Content**

**Vulnerability Severity Definitions**

**Critical**
If exploited, an attacker will gain complete control of the asset. Critical level vulnerabilities are known to have publicly accessible exploits which require little to no expert knowledge to use. In some cases, the presence of critical-level vulnerabilities indicate that the asset has already been compromised. Immediate action must be taken to resolve these vulnerabilities.

**High**
If exploited, an attacker could gain user or administrative access to the asset and be able to run commands, access or delete files, and launch attacks against other assets. High-level vulnerabilities often require some expert knowledge to exploit and publicly accessible exploits may not be available. These vulnerabilities should be resolved as soon as possible.

**Medium**
If exploited, an attacker would gain valuable information about the asset, which would aid in gaining access. In many cases, Medium-level vulnerabilities are a result of improperly configured Services, weak or absent security configurations, or unprotected limited access accounts. These vulnerabilities should be dealt with reasonably quickly.

**Low**
If exploited, an attacker could gain information about the asset but it would not necessarily lead to access. Low-level vulnerabilities can usually be addressed by applying security hardening practices or disabling services.

**Trivial**
If exploited, an attacker could gain information about the asset but it should not lead to access. In many cases trivial-level vulnerabilities have no possible solution due to operating system limitations, and pose a minimal risk to asset security.

**Information**
Information provided by an asset or a service that is not considered a vulnerability.

**Scanning Remediation**

Information Technology Services scans all university-owned computers daily. Any vulnerabilities discovered during a security assessment will be corrected by the system administrator responsible for the asset and a retest will be performed to validate that the identified vulnerability has been appropriately remediated or mitigated.

Critical risk vulnerabilities will be removed from the network and remediated before placed back on the network. High risk vulnerabilities must be remediated or mitigated within 24 hours of being reported to the system administrator. Medium, Low, and Trivial risk vulnerabilities will be evaluated based on the type of host and function.

**Revision Management**

**Revision History Log:**

<table>
<thead>
<tr>
<th>Revision #:</th>
<th>Date:</th>
<th>Recorded By:</th>
</tr>
</thead>
<tbody>
<tr>
<td>v2.0</td>
<td>8/21/2020 8:02 AM</td>
<td>Holly Warfel</td>
</tr>
<tr>
<td>v1.0</td>
<td>1/14/2020 2:46 PM</td>
<td>Courtney Cunningham</td>
</tr>
</tbody>
</table>

**Vice President Approval:**
Enter Vice President(s) that are responsible for approving this document

<table>
<thead>
<tr>
<th>Name:</th>
<th>Title:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gary Logan</td>
<td>Vice President for Finance &amp; Administration</td>
</tr>
</tbody>
</table>