Information Technology Services
Security Control Standards

NIST Control Family – System and Information Integrity

<table>
<thead>
<tr>
<th>CONTROL NUMBER</th>
<th>CONTROL NAME</th>
<th>PRIORITY</th>
<th>REVISION DATE</th>
<th>NEXT SCHEDULED REVIEW DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SI-3</td>
<td>Malicious Code Protection</td>
<td>P1</td>
<td>4/15/2020</td>
<td>4/15/2021</td>
</tr>
</tbody>
</table>

I. **Statement**
Tarleton shall employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; updates malicious code protection mechanisms whenever new releases are available in accordance with University configuration management policy and procedures; configures malicious code protection mechanisms to perform periodic scans of the information systems. The code protection shall also take automated actions against any malicious code that is found.

II. **Applicability**
This Control applies to all Tarleton network information resources. The intended audience for this Control includes all information resource owners, custodians, and users of information resources.

III. **Risk Statement**
Unauthorized, malicious code is executed on systems without authorization.

IV. **Implementation**
All University information resources use a centrally administered anti-malware application/service/utility to detect and eradicate or quarantine malicious code.