ISO Position Paper

<table>
<thead>
<tr>
<th>Position Title</th>
<th>Data Transmission and Encryption Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position Audience</td>
<td>Princeton IT Professionals</td>
</tr>
<tr>
<td>Contact</td>
<td>Information Security Office: <a href="mailto:InfoSec@princeton.edu">InfoSec@princeton.edu</a></td>
</tr>
<tr>
<td>Position Release Date</td>
<td>November 2018</td>
</tr>
<tr>
<td>Last Update</td>
<td>Initial posting</td>
</tr>
</tbody>
</table>

**Problem Statement**

Data transmission and encryption standards continue to evolve as new weaknesses and vulnerabilities are discovered. Devices that are not properly maintained could lead to exploitation by bad actors and, as a result, could put Princeton University information at risk.

**ISO Position**

All University servers and devices including development, QA, and production, should be configured using the latest recommended standards. These standards include the following:

- a current SHA2 certificate issued by the University certificate service
- use of TLS 1.1 and above
- strong ciphers
- no use of SSL 2.0 and SSL 3.0

**Additional Information**

- Certificates: How to request a digital certificate for a web server at Princeton University
- InCommon Certificate Use for SSL/TLS position paper
- Self-signed Web Server Certificates position paper

Information Security Office
Princeton University

Data classification: Public