I. PURPOSE

The purpose of this policy is to require the acquisition, installation, use and maintenance of digital (aka SSL/TLS\(^1\)) certificates in certain Internet communications involving endpoint browsers and websites.

Digital certificates create secure (i.e., encrypted) links between websites and a visitor's browser. A digital certificate that is signed by a valid certificate authority (CA):

- Verifies the identity of the server to the client (i.e. the client is connecting to the real <example>.uky.edu), and
- Is used to encrypt data in both directions between the client (i.e., the browser) and the server (that hosts the website).

II. APPLICABILITY

This policy is applicable to all personnel who have or are responsible for securing communications between a UK website and an Internet browser (i.e., Internet Explorer, Chrome, Firefox, etc.) and all UK systems, applications, appliances or web sites that use the LinkBlue ID/password combination for purposes of authentication, or that transmit/receive confidential data.

III. POLICY

Any University system, application, appliance or site that uses the LinkBlue ID/password combination for purposes of authentication, or that transmits/receives data classified as confidential shall:

1. Employ Transport Layer Security (TLS) or an equivalent-or-stronger cryptographic protocol for authenticating and establishing identities, and maintaining encrypted communications channels between endpoints; and

2. Use a Secure Hypertext Transport Protocol (HTTPS) connection based on server-side, digital certificates signed by a recommended trusted third-party certificate provider.

Note: The University of Kentucky has partnered with the InCommon Certificate Service\(^2\) to provide unlimited digital certificates signed by root CA (Certificate Authority) provider Comodo to all of UK at no additional cost\(^3\).

What kind of certificates are available?

The following certificates/products are available via the InCommon Certificate Service:

- Standard SSL/TLS Server certificates
- Multi-Domain SSL Certificates
- Wildcard certificates (some restrictions apply)
- Extended Validation (EV) Certificates Upon request
- Code-signing certificates
- Intranet SSL certificates (will be discontinued after October 31, 2015)

---

\(^1\) SSL: Secure Sockets Layer. TLS: Transport Layer Security. SSL is no longer considered secure and its use is not recommended.

\(^2\) www.incommon.org/certificates/

\(^3\) For additional information and process for acquiring these certificates: www.uky.edu/ukit/security/certs
IV. DEFINITIONS  (not complete)

V. REFERENCES

VI. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Primary Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/23/14</td>
<td>Initial draft developed</td>
<td>M. Carr</td>
</tr>
</tbody>
</table>