# Server Side Certificate Policy

## Overview

The need to communicate securely over public networks resulted in the development of the Public Key Infrastructure (PKI) framework. PKI utilizes public-key cryptography and digital certificates to enable data to be sent in a secure and confidential manner. These technologies help secure and encrypt data transmissions between client and servers during browser-based communications.

Certificates are most commonly used for secure website applications or Secure Hypertext Transport Protocol (HTTPS) transmissions. Web browsers inspect signed server-side certificates to verify that a web server is authentic, using a specific URL, and that the URL has been publicly verified with the identity of the institution. Using a server certificate helps assure the integrity and confidentiality of the encrypted communications through the use of cryptographic protocols such as Transport Layer Security (TLS).

## **Purpose**

Certificate Authorities (CA) sign and distribute certificates used to ensure an identity when establishing encrypted communications. Controls are in place to select providers of trusted server-side third-party certificates and their implementation within [LEP] [Insert Applicable Department] architecture and application development.

## Scope

This policy applies to all [LEP] staff who create, deploy, or support application, system and web server software.

## Policy

### GENERAL

[LEP] [Insert Applicable Department] shall ensure server side security controls protect sensitive communications by encrypting communication channels between endpoints using TLS or equivalent cryptographic protocols. Secure Hypertext Transport Protocol (HTTPS) connections based on server-side certificates shall be signed by a trusted third-party certificate provider. Where possible, the latest versions of TLS shall be used to protect authentication and communications against eavesdropping and tampering.

### PROCESS AND PROCEDURES

Certificate solutions shall be installed and maintained according to the provider’s instructions and recommended use. Any deviation from the provider’s instructions or recommended use must be approved by the [Insert Applicable Role] or their designee.

The following procedures shall be implemented related to certificate usage and management:

* Network administrators shall track certificate expiration dates and ensure certificates are kept current
* Self-signed certificates are only permitted for development systems that are segregated from the [LEP] production network and are not connected to external public resources
* Network administrators shall comply with the [LEP] Server Hardening Policy to ensure systems are protected from security and performance issues.
* The use of wildcard certificates for one or more subdomains within [LEP] is permissible only under the following conditions:
  + The service provided by the system may not be used to store or access sensitive data
  + All requests for wildcard certificates are approved by the [Insert Applicable Role] prior to certificate purchase, acquisition, or assignment

## Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the [LEP] procedures. Examples of proper controls and documentation include:

* A current server side certificate log annotating certificate provider, initiation date, expiration date, and applications served
* Documentation of any wildcard certificates and their reasons for use

## Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

## Distribution

This policy is to be distributed to all [LEP] staff and contractors supporting web application and infrastructure delivery servers.

## Policy Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 11/15/2016 | Initial Policy Drafted |  |
|  |  |  |  |
|  |  |  |  |