

9300-P010 – Web SSL Certificate Use Policy

I. PURPOSE

The purpose of this policy is to establish the requirements for use of SSL (Secure Sockets Layer) Certificates on web sites and web applications.

II. SCOPE

This policy applies to all web sites and web applications of Executive Branch agencies, boards, and commissions.

III. POLICY

- A. Any web site or web application that requires authentication through the use of user ID's, passwords, pin numbers, etc. must use SSL encryption on the pages utilizing authentication.
- B. Any sensitive data transmitted over the internet must use SSL. Sensitive information may include:
 - Social Security Number, Employer Identification Number, or other account identifiers; or
 - Date of birth; or
 - Phone number for a person or business; or
 - Street address for a person or business; or
 - Employment and wage information; or
 - Health information; or
 - Other information defined by law as confidential, sensitive, or non-public information
- C. At a minimum, web pages providing user authentication using SSL must display the certificate vendor's secure site seal on the login page.
- D. Only valid third-party SSL certificates can be used on public access pages that require SSL.
- E. Intranet pages that require SSL can use either third-party SSL certificates, or internally generated certificates.
- F. A minimum of 128 bit encryption is required for SSL certificates.

CIO Approved Date: 12/16/2009