

Security Best Practices:

Best Practice 1. Resetting security assurance levels should not require modification of the architecture.

Best Practice 2. Provide infrastructure security services to enable the enterprise to conduct business electronically.

Best Practice 3. An accurate system date and time are essential to all security functions and accountability and must be maintained.

Best Practice 4. Perform a business-driven risk assessment for all automated systems.

Best Practice 5. When designing collaborative systems (e.g. document management, workflow), the content that will move through the system must be classified according to applicable statutes, policies and regulations pertaining to availability, retention

A privacy policy should be published on every government web site, even if the site does not create records of the information collected. Because state agency web sites have many different purposes, the privacy policies found on these sites should also be diverse and specific to the visited site. A policy should have an *introductory statement* that identifies the agency and includes a short overview of privacy practices and how they apply to the site. In the course of operating a web site, certain information may be collected automatically in logs or by cookies. Agencies may have the technical ability to collect information and later take additional steps to identify people, such as looking up static Internet Protocol addresses that can be linked to specific individuals. The privacy statement must clearly denote the policy. It is imperative to ensure these policies are consistent with the State's **Freedom of Information laws.**

Best Practice 6. Utilize Defense in Depth practices to create a multi-level, multi-layer construct to protect State of Connecticut assets. (Example: harden servers, use a multi-tier firewalls, host and network based intrusion prevention appliances, router access control lists, encryption, anti-virus, anti-malware etc.)

Best Practice 7. Apply a level of security to resources commensurate to its value to the organization and sufficient to contain risk to an acceptable level.

Best Practice 8. Treat security architecture as a continuous process.

Best Practice 9. Locate security in the appropriate layer of a communications protocol to ensure maximum usability with minimum future modification.

Best Practice 10. Use commercially generated certificates when encryption is needed and where there will be a direct interaction with a user's browser or client software. The browser or client software will accept this as a valid certificate without question. Use non-commercial or self generated certificates between machines to ensure the data stream is encrypted, but the certificate will not be verified or questioned by a certificate authority. This reduces TCO of using certificates while providing confidence to the user that the connection is a verifiable certificate and the encryption level.