CHAPTER 23

SECURITY AND USE OF DIGITAL CERTIFICATES

PURPOSE:

This chapter establishes the requirements for the security and use of digital certificates within the Department's information technology infrastructure.

AUTHORITY:

Sections 20.23(3)(a) and 334.048(3), Florida Statutes (F.S.)

REFERENCES:

Chapter 21 of this Manual

Formatted: Space After: 0 pt, Line spacing: single

Section 668.50(h), F.S., and Section 668.003(1)(a)-(d), F.S.

Chapter 815, F.S., Computer Related Crimes

Procedure No. 250-012-011, Disciplinary Actions

Rules 60L - 36.005, 71A-1.018(1) and 74-2, Florida Administrative Code (F.A.C.)

SCOPE:

The provisions of this chapter apply to all units within the Department.

23.1 Use of Digital Certificates

It is the intent of the Department to streamline processes and create efficiencies via the use of digital certificates and electronic signatures. Pursuant to Florida law, an electronic signature "means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record," section ***668.50(h), F.S***. A digital certificate "means a computer-based record which: identifies the certificate authority, identifies the subscriber, contains

the subscriber's public key, [and] is digitally signed by the certification authority," section ***668.003(1)(a)-(d), F.S.***

23.1.1 The use of digital certificates and electronic signatures within the Department shall be governed in accordance with the provisions of Department policies, procedures, handbooks, and manual chapters governing such use, as well as Florida law. Unless otherwise provided by law, an electronic signature may be used to sign a writing and shall have the same force and effect as a written signature. If Department policy or Florida law requires the notary of a signature or record, the authorized and legal notary may use an electronic signature to satisfy the notary requirement so long as all legally required information is attached to or logically associated with the signature or record.

23.1.2 The use of digital certificates and electronic signatures shall be consistent with reasonable practices concerning electronic transactions and with the continued expansion of those practices. ***Chapter 21 of this Manual, Acquiring and Managing Digital Certificates*** establishes the procedural requirements for the acquisition, management, and revocation of digital certificates, including those digital certificates used for electronic signatures.

23.1.3 Digital certificates shall only be used by the individual to whom the digital certificate is assigned (the digital certificate holder). Digital certificate holders may not grant the use of his or her assigned digital certificate for use by others, including delegates. Delegates authorized to affix electronic signatures on behalf of a delegator shall have assigned to him or her, his or her own digital certificate for that stated purpose. Further, delegates shall refuse the receipt of a digital certificate that is not specifically assigned to him or her.

23.1.4 Digital certificate holders shall not use digital certificates for other than the certificate's stated or implied purpose.

23.1.5 The implementation of digital certificates for specific processes requires Senior Management Service (SMS) or Traditional Select Exempt Service (SES) level approval. Further, third parties must agree to conduct business transactions via an electronic means prior to the implementation of digital certificates. At any time, any party engaged in electronic transactions may withdraw previously provided agreement to conduct business electronically. "Whether the parties agree to conduct transactions electronically is determined from the context and surrounding circumstances, including the parties' conduct," ***668.50(5)(b), F.S.***

23.1.6 Prior to the implementation of digital certificates, the District or Central Office unit seeking to implement the use of digital certificates shall complete a ***Digital Certificate Security Assessment***. Content requirements for the ***Digital Certificate Security Assessment*** are specified in ***Chapter 21, section 21.2.1 of this Manual***.

23.2 Procurement of Digital Certificates

23.2.1 Centralized Procurement of Digital Certificates

Procurement of digital certificates shall be centralized within the Office of Information Technology (OIT). District and Central Office units seeking to procure digital certificates shall complete a **Digital Certificate Security Assessment**. The requesting District or Central Office unit shall reimburse OIT for all digital certificates purchased on behalf of the District or Central Office unit. For digital certificate procurement processed through OIT, refer to ***Chapter 21, section 21.1.1.***

23.2.2 Authorized Vendors

OIT shall maintain and publish a list of authorized vendors for digital certificates. This list shall be incorporated into the ***Department's Standards List***, as specified in ***Chapter 8 of this Manual***.

23.3 Security of Digital Certificates

23.3.1 Digital Certificate Holders Requirements

Digital certificate holders are responsible for the following:

a. Protecting the digital certificate from unauthorized use
b. Using the digital certificate for only the stated or implied use
c. Protecting any passwords associated with the digital certificate from unauthorized disclosure
d. Assuring that the digital certificate assigned to a digital certificate holder is only installed and used on Department owned or leased information technology resources
e. Timely notification of the need to renew an assigned digital certificate to the appropriate digital certificate coordinator
f. Immediately reporting suspected breaches of security as specified in ***Chapter 1 of this Manual***
g. Backing up the digital certificate as specified in section ***23.4 of this Chapter***

h. Timely submittal of an Automated Access Request Form requesting the revocation of the digital certificate once digital certificate is no longer needed.

23.3.2 Requesting a Digital Certificate

Users requiring a digital certificate shall request the digital certificate via the AARF System. Upon the approval of the AARF request, it is the responsibility of the Enterprise Technology Services and Support team to acknowledge or reject the request, and to assist the user with obtaining the required digital certificate.

23.3.3 Revoking and Purging a Digital Certificate

Regardless of cause, when a digital certificate holder no longer requires access to an assigned digital certificate, the user's Supervisor shall ensure that an AARF Request is submitted to request the removal of the digital certificate. Upon receipt of the approved AARF Request, the Enterprise Technology Services and Support Team shall submit a request to the Certificate Authority to revoke the certificate.

Revoked digital certificates shall be purged from all systems upon which the certificate is installed in accordance with the requirements established in section ***23.3.1(h) of this Chapter.***

23.4 Backing-up of Digital Certificates

Backup of the digital certificate is the responsibility of the digital certificate holder. The backup file shall be placed on a Department network share to which the holder has access. The backup of the digital certificate shall be password protected. The digital certificate holder shall protect the backup file and associated password from unauthorized access and disclosure.

23.5 Compliance

Misuse or abuse of digital certificates is subject to the Department's disciplinary standards, up to and including immediate dismissal, civil penalties, or criminal penalties. Refer to the Department's ***Disciplinary Standards*** contained in ***Rule 60L-36.005, F.A.C.,*** and the ***Disciplinary Action Procedure, Topic No.: 250-012-011***. Failure to comply with related department policies, procedure, and standards may lead to termination of contracts for contractors, partners, consultants and other entities that provide service to the Department. Furthermore, pursuant to ***Chapter 815, F.S., Computer Related Crimes***, all individuals who violate these related statutes, rules, policies, procedures, and standards, are subject to possible legal (civil, or criminal, or both) prosecution. The purchase and use of digital certificates is governed via related

Florida Statutes, Florida Administrative Code, and Department policies and procedures, especially ***Acquiring and Managing Digital Certificates*** found in ***Chapter 21*** of ***this Manual***.

TRAINING:

None Required.

FORMS:

None Required.