18 NCAC 10 .0306 PUBLIC KEY TECHNOLOGY: PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

(a) Physical Security -- Access Controls.

(1) The Certification Authorities, and all Registration Authorities, Certificate Manufacturing Authorities and Repository Services Providers, shall implement physical security controls to restrict access to hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing Certification Authority Services. Access to such hardware and software shall be limited to personnel performing in a Trusted Role as described in this Rule. Access shall be controlled through the use of electronic access controls, mechanical combination lock sets, or deadbolts. Such access controls must be manually or electronically monitored for unauthorized intrusion at all times.

(2) Breach of physical security or access control expectations may result in revocation of the Certification Authority's license.

(b) Procedural Controls.

(1) Trusted Roles. All employees, contractors, and consultants of a Certification Authority (collectively "personnel") having access to or control over cryptographic operations that may materially affect the Certification Authority's issuance, use, suspension, or revocation of certificates shall, for purposes of the rules in this Chapter, be considered as serving in a trusted role. This includes access to restricted operations of the Certificate Authority's repository. Such personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who are designated to oversee the Certification Authority's operations.

(2) Multiple Roles (Number of Persons Required Per Task). To ensure that one person acting alone cannot circumvent safeguards, multiple roles and individuals shall share Certification Authority server responsibilities. Each account on the Certification Authority server shall have limited capabilities commensurate with the role of the account holder.

(c) Personnel Security Controls.

(1) Background and Qualifications. Certification Authorities, Registration Authorities, Certificate Manufacturing Authorities and Repository Service Providers shall formulate and follow personnel and management policies sufficient to provide assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in manner consistent with the rules in this Chapter.

(2) Background Investigation.

(A) Certification Authorities shall conduct a background investigation of all personnel who serve in trusted roles (prior to their employment and at least every five years thereafter) to verify their trustworthiness and competence in accordance with the requirements of the rules in this Chapter and the Certification Authority's personnel Practice Statements or their equivalent. All personnel who fail an initial or periodic investigation shall not serve or continue to serve in a trusted role.

(B) Operative personnel shall not ever have been convicted of a felony or a crime involving fraud, false statement or deception.

(C) Any civil or administrative findings involving fraud, false statement or deception involving operative personnel must be disclosed.

(3) Training Requirements. All Certification Authority, Registration Authority, Certificate Manufacturing Authority and Repository Services Provider personnel must receive training in order to perform their duties, and update briefings thereafter as necessary to remain current.

(4) Documentation Supplied to Personnel. All Certification Authority, Registration Authority, Certificate Manufacturing Authority, and Repository Services Provider personnel must receive comprehensive user manuals detailing the procedures for certificate creation, update, renewal, suspension, revocation, and software functionality.

History Note: *Authority G.S. 66-58.10;*
Temporary Adoption Eff. February 23, 1999;
Codifier determined on November 23, 1999, agency findings did not meet criteria for temporary rule;
Temporary Adoption Eff. December 3, 1999;
Eff. March 26, 2001;

Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. December 6, 2016.