

§ 11.200

21 CFR Ch. I (4–1–03 Edition)

§ 11.200 Electronic signature components and controls.

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

§ 11.300 Controls for identification codes/passwords.

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

PART 12—FORMAL EVIDENTIARY PUBLIC HEARING

Subpart A—General Provisions

Sec.

12.1 Scope.

Subpart B—Initiation of Proceedings

12.20 Initiation of a hearing involving the issuance, amendment, or revocation of a regulation.

12.21 Initiation of a hearing involving the issuance, amendment, or revocation of an order.

12.22 Filing objections and requests for a hearing on a regulation or order.

12.23 Notice of filing of objections.

12.24 Ruling on objections and requests for hearing.

12.26 Modification or revocation of regulation or order.

12.28 Denial of hearing in whole or in part.

12.30 Judicial review after waiver of hearing on a regulation.

12.32 Request for alternative form of hearing.

12.35 Notice of hearing; stay of action.

12.37 Effective date of a regulation.

12.38 Effective date of an order.

Subpart C—Appearance and Participation

12.40 Appearance.

12.45 Notice of participation.

12.50 Advice on public participation in hearings.

Subpart D—Presiding Officer

12.60 Presiding officer.

12.62 Commencement of functions.

12.70 Authority of presiding officer.

12.75 Disqualification of presiding officer.

12.78 Unavailability of presiding officer.